

CODE OF BUSINESS CONDUCT AND ETHICS

ICD'S VISION

By 2024, ICD will be widely recognized as the key catalyst in effecting positive change in the corporate governance ecosystem for inclusive and sustainable development.

ICD'S MISSION

To advocate good governance and stewardship in the corporate sector for the benefit of society.

ICD'S VALUES

Independence, Patriotism, Integrity and Ethics, Excellence, Solidarity, Social Responsibility

The INSTITUTE OF CORPORATE DIRECTORS of the PHILIPPINES ("ICD" or "INSTITUTE"), pursuant to its MISSION "To advocate good governance and stewardship in the corporate sector for the benefit of society," is fully committed to its corporate affairs in accordance with long held values and ethical standards that have been the foundation of its advocacy and in inviting Fellows and members to its Society.

In order to promote and realize its CORE VALUES of Independence, Patriotism, Integrity & Ethics, Excellence, Solidarity, and Social Responsibility, the INSTITUTE formally adopts the CODE OF BUSINESS CONDUCT AND ETHICS by specifying the behaviors and practices that are expected from Trustees, Officers and staff. It seeks to create awareness and form an important building block of its corporate culture. It is important that all are aware of these values and behaviors and should there be non-compliance, the offending person will face the appropriate consequences.

I. COVERAGE OF THE CODE

This Code of Business Conduct and Ethics states the principles that guide ICD's Trustees, Officers and Employees in the performance of their duties and responsibilities, and in their transactions with the Fellows and other members, partners and collaborators, creditors, customers, contractors, suppliers, regulators, and the general public.

Partners and collaborators, creditors, customers, contractors, suppliers, and other stakeholders should align their dealings with ICD's Code of Business Conduct and Ethics.

Trustee, Fellows and Members shall follow this code in relation to their dealings with the regular Officers and Employees, or in their participation in the programs of the INSTITUTE. Fellows and other members of the ICD are also covered by this Code insofar as they participate in the teaching and consultancy programs of the INSTITUTE.

The Code has the following Chapters and Annexes:

- I. Coverage of the Code of Business Conduct and Ethics
- II. Compliance with Laws
- III. Ethical Conduct and Practices IV. Officers' and Employees' Welfare
- IV. Accountability, Integrity and Vigilance; Whistleblower Program
- V. ANNEXES:

Annex A – Data Privacy Policy

Annex B – Policy on Related Party Transactions

Annex C – Policy and Procedures in Conflict of Interest Situations

Annex D – Guidelines on Acceptance of Gifts

Annex E – Guidelines on Travel sponsored
by a Business or Program Partner

Annex F – Disciplinary Procedures and Penalties for Violation
of the Code of Business Conduct and Ethics

Annex G – Procedures for Reporting and Investigating Harassment

II. COMPLIANCE WITH LAWS

ICD's business and advocacy dealings shall be compliant with all applicable laws in the countries and communities in which it operates. This includes legislation and regulation pertaining to financial reporting, upholding fair trade and competition, pricing, employment, data privacy, protection of the environment and other regulations.

A. Data Privacy

ICD collects, processes and stores personal data of persons who, and entities which, avail of its programs, products and services, including its websites and mobile applications, participate in their events, apply for a job with them, or enter into any contract with them, provided that such persons or entities have given their express consent. ICD's **Data Privacy Policy (Annex A)** has been prepared inform any person who avails of the programs and services of ICD on how their personal data are being collected, used and secured.

B. Public Disclosures

ICD shall maintain accurate and complete records of all financial and business transactions in accordance with laws and regulations governing financial reporting and generally accepted accounting principles. These provide the basis for the report it discloses to the public, BIR and SEC and other stakeholders regarding ICD's results of operations and financial position. ICD also ensures that an independent audit of its financial statements is conducted by reputable external auditors.

C. Related Party Transactions

Full disclosure of the details, nature, extent, and all other material information on transactions with related parties shall be observed in the ICD's financial statements and annual reports to the SEC.

ICD Management shall present the details of transactions entered into by the INSTITUTE with related parties to the Audit Committee for review in accordance with ICD's **Related Party Transactions Policy (Annex B)**. This is to ensure that the ICD conducts all related-party transactions at arm's length. When acting as Related Party Committee, the Audit Committee may invite other Trustees to participate in its meetings as experts.

III. ETHICAL CONDUCT AND PRACTICES

In addition to compliance with laws and regulations, ICD supports ethical practices in the way it conducts business and pursues its advocacy programs, as follows:

A. Support for Diversity and Non-Discrimination

Whether in selection of the communities and markets where ICD operates, partnering with other advocacy groups or multilateral agencies, hiring and promotion of employees, selection of suppliers and contractors – the INSTITUTE decides on the basis of merit and value to the Fellows and other members, and other stakeholders, and does not discriminate on the basis of race, ethnicity, religion or gender.

Trustees, Officers and Employees of the INSTITUTE are prohibited from practicing any form of discrimination or harassment in the workplace. This obligation to refrain from such behavior extends to contractors, vendors, suppliers, or visitors, to the extent that their conduct affects the work environment.

B. Respect for Confidentiality and Privacy of Information

Trustees, Officers and Employees are expected to safeguard information relating to ICD, its program partners, as well as its clientele. Financial reports, strategies, and plans shall not be disclosed to third parties unless authorized by ICD or required by law. Information regarding individuals working for ICD shall also be treated as private information and shall not be divulged to other parties except when required by legal processes or with the consent of the employee.



C. Members and Clientele Welfare

ICD recognizes that the core of its business is primarily to promote the best interests and ideals of its Fellows and other members, its clientele, and values their satisfaction and loyalty. Thus, all Trustees, Officers and Employees shall be guided by fairness, professionalism, courtesy and respect when dealing with Fellows and other members, program partners and clientele, and shall endeavor to provide excellent and diligent service at all times. No false or misleading information shall be provided to any of such stakeholder. Likewise, ICD is committed to protect the safety and security of its Fellows and other members, its clientele and program partners. Accordingly, the INSTITUTE shall undertake to keep its premises well-secured, and continuously implement ways to eliminate hazards that would pose threats to the safety of its Fellows and other members and clientele.

D. Policy on Conflicts of Interests

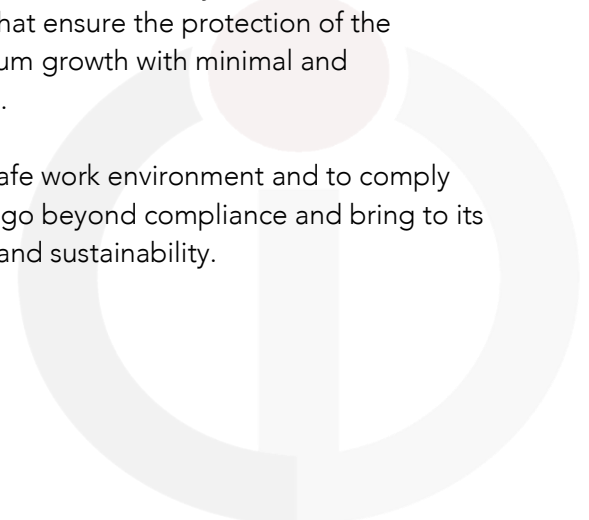
Conflict of interest situations may cast doubt on the integrity and fairness of ICD's business transactions. Under its **CORE VALUES** of **Independence, Integrity** and **Ethics**, ICD is committed to ensure that the best interest of the INSTITUTE, its Fellows and other members, and its advocacy programs, is not made secondary to personal interests of its Trustees, Officers and/or Employees. Transparency with regard to real or perceived conflict of interest also protects the personal integrity of ICD Trustees, Officers and Employees involved. The policy preserves the trust of ICD Board and Management that all Trustees, Officers and Employees abide by the authority and privileges granted for what is best for the INSTITUTE. Annex C provides details of the policy and procedures to be followed.

All business decisions and actions must be based on the best interests of the INSTITUTE and the value to Fellows and other members, and should not be motivated by personal considerations or relationships which may interfere with the exercise of independent judgment.

E. Corporate Social Responsibility

ICD shall initiate and participate in charitable causes and community organizations to improve the quality of life of the communities where it operates, through education, health care and livelihood programs. Environmental and Safety Practices ICD shall endeavor to adhere to sustainable practices that ensure the protection of the environment, and shall seek to deliver maximum growth with minimal and responsible consumption of natural resources.

The INSTITUTE is committed to providing a safe work environment and to comply with all environmental regulations. It seeks to go beyond compliance and bring to its markets best practices in environmental care and sustainability.



IV. OFFICERS' AND EMPLOYEES' WELFARE

All Officers and Employees are to be selected, engaged, and compensated based on qualification and performance. They shall be treated fairly and accorded respect and dignity. Their individual and collective rights shall not be violated.

ICD shall maintain a safe, productive and conducive workplace and comply with all applicable health, safety and environmental laws. In this regard, Officers and Employees are covered by rules against the use of prohibited drugs, working under the influence of liquor, or engaging in gambling in the workplace.

Opportunities for career advancement shall be provided based on clear performance and qualifications criteria, which shall include both financial and non-financial measures. ICD shall also provide learning and development opportunities for professional growth.

A. Discrimination Is Prohibited

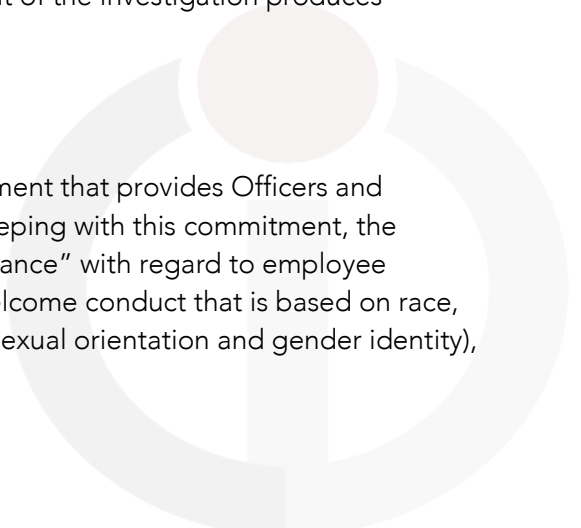
ICD is an equal opportunity employer and makes all employment decisions without regard to race, religion, skin color, sex (including pregnancy, sexual orientation and gender identity), national origin, disability, age, genetic information, or any other status protected under applicable laws. This policy applies to all terms and conditions of employment, including but not limited to, hiring, placement, promotion, termination, layoff, recall, transfers, leaves of absence, benefits, compensation and training. The INSTITUTE seeks to comply with all applicable laws related to discrimination and will not tolerate the interference with the ability of any of ICD's Officers and Employees to perform their job duties.

ICD makes decisions concerning employment based strictly on an individual's qualifications and ability to perform the job under consideration, the comparative qualifications and abilities of other applicants or employees, and the individual's past performance within the organization.

Any Trustee, Officer or Employee who believes that an employment decision has been made that does not conform with Management's commitment to equal opportunity, should promptly bring the matter to the attention of the Whistleblowing coordinator. The complaint shall be promptly, thoroughly and impartially investigated. There will be no retaliation against a Trustee, Officer or Employee who files a complaint in good faith, even if the result of the investigation produces insufficient evidence to support the complaint.

B. Zero Workplace Harassment

ICD is committed to providing a work environment that provides Officers and Employees equality, respect and dignity. In keeping with this commitment, the INSTITUTE has adopted a policy of "zero tolerance" with regard to employee harassment. Harassment is defined as an unwelcome conduct that is based on race, skin color, religion, sex (including pregnancy, sexual orientation and gender identity),



national origin, age (40 or older), disability or genetic information. Harassment becomes unlawful where:

- (1) enduring the offensive conduct becomes a condition of continued employment; or
- (2) the conduct is severe or pervasive enough to create a work environment that a reasonable person would consider intimidating, hostile, or abusive.

This policy applies to all aspects of employment. Harassment of any other person, including, without limitation, fellow employees, contractors, visitors, clients or customers, whether at work or outside of work, is grounds for immediate termination. The INSTITUTE will make every reasonable effort to ensure that its entire community is familiar with this policy and that all employees are aware that every complaint received will be promptly, thoroughly and impartially investigated, and resolved appropriately. ICD will not tolerate retaliation against anyone who complains of harassment or who participates in an investigation.

C. Sexual Harassment

Sexual harassment has been declared unlawful under Republic Act 7877, and applies equally to men and women. The law defines sexual harassment as unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature, when the conduct:

- (1) explicitly or implicitly affects a term or condition of an employee's employment;
- (2) is used as the basis for employment decisions affecting the employee; or
- (3) unreasonably interferes with an employee's work performance or creates an intimidating, hostile or offensive working environment.

Such conduct may include, but is not limited to: subtle or overt pressure for sexual favors; inappropriate touching; lewd, sexually oriented comments or jokes; foul or obscene language; posting of suggestive or sexually explicit posters, calendars, photographs, graffiti, or cartoons; and repeated requests for dates. ICD policy further prohibits harassment and discrimination based on sex stereotyping.

Sex stereotyping occurs when one person perceives a man to be unduly effeminate or a woman to be unduly masculine and harasses or discriminates against that person because he or she does not fit the stereotype of being male or female.

The INSTITUTE encourages reporting of all perceived incidents of sexual harassment, regardless of who the offender may be. Every employee is encouraged to raise any questions or concerns with the Whistleblowing coordinator.

D. Supervisors' Responsibilities

All managers or supervisors are expected to ensure that the work environment is free from sexual and other harassment. They are responsible for the application and communication of this policy within their work areas. Managers and supervisors should:

- Encourage employees to report any violations of this policy before the harassment becomes severe or pervasive.
- Make sure the Human Resources Department is made aware of any inappropriate behavior in the workplace.
- Create a work environment where sexual and other harassment is not permitted.

E. Drug-Free Workplace

The INSTITUTE takes the problem of drug and alcohol abuse seriously, and is committed to providing a substance abuse-free workplace for its Officers and Employees. Substance abuse of any kind is inconsistent with the behavior expected of Trustees, Officers and Employees, subjects all employees and visitors to ICD's facilities to unacceptable safety risks, and undermines our ability to operate effectively and efficiently.

The INSTITUTE recognizes alcohol and drug abuse as potential health, safety and security problems. ICD expects all Officers and Employees to assist in maintaining a work environment free from the effects of alcohol, drugs or other intoxicating substances. Compliance with this substance abuse policy is made a condition of employment, and violations of the policy may lead to discipline and/or discharge.

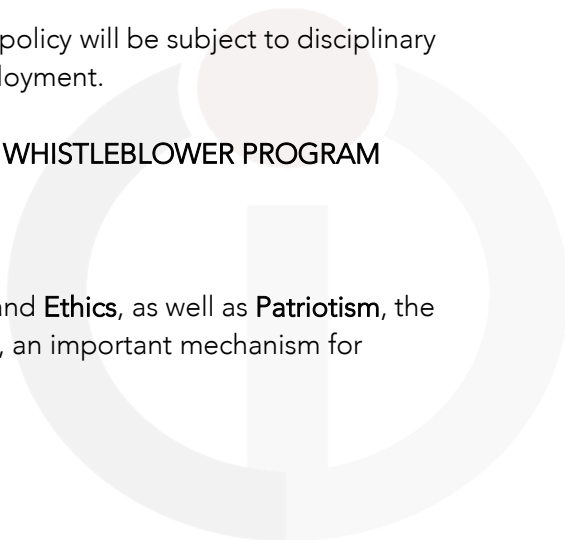
Officers and Employees are prohibited from engaging in the unlawful manufacture, possession, use, distribution or purchase of illicit drugs, alcohol or other intoxicants, as well as the misuse of prescription drugs on ICD premises or at any time and any place during working hours. While the INSTITUTE cannot control behavior off the premises, it encourages all Officers and Employees to behave responsibly and appropriately at all times. All Officers and Employees are required to report to their jobs in appropriate mental and physical condition, ready to work.

Any person who violates this substance abuse policy will be subject to disciplinary action up to and including termination of employment.

V. ACCOUNTABILITY, INTEGRITY AND VIGILANCE; WHISTLEBLOWER PROGRAM

A. Rationale and General Policy

In pursuit of ICD's **CORE VALUES** of **Integrity** and **Ethics**, as well as **Patriotism**, the INSTITUTE supports a **Whistleblower Program**, an important mechanism for



preventing and detecting fraud, malpractices or misconduct, and enabling fast and coordinated incident responses to establish cause, remedial actions, and damage control procedures.

All Officers and Employees, as well as partners, customers, suppliers, service providers and all other stakeholders, may report any real or perceived violation of ICD policies, procedures and applicable laws and regulations which include, but are not limited to, Alcohol-Free Workplace Policy and Program, Policy on Sexual Harassment in the Workplace, Policy on Drug-Free Workplace, Conflict of Interest, Corruption, Code of Business Conduct and Ethics policies and other rules and regulations.

B. Reporting Mandate

It is the responsibility of all Trustees, Officers and Employees, and expected as well from ICD's partners, customers, suppliers, service providers and all other stakeholders to comply with and to report violations or suspected violations of the Code of Business Conduct and Ethics policies or laws in accordance with this policy.

ICD will appoint a Whistleblowing coordinator. Upon receipt of the whistleblower report, the coordinator shall immediately initiate the investigation and shall follow due process in handling fraud and irregularities. The findings will be reported to the Board for consideration, without the identity of the whistleblower being divulged. After giving the suspected perpetrator a chance to prove his innocence, the Board will decide what corrective action is required vis-à-vis the perpetrator. The Audit Committee will subsequently review whether additional or tighter internal controls are required to make repeat of this incident unlikely.

C. Reporting in Good Faith

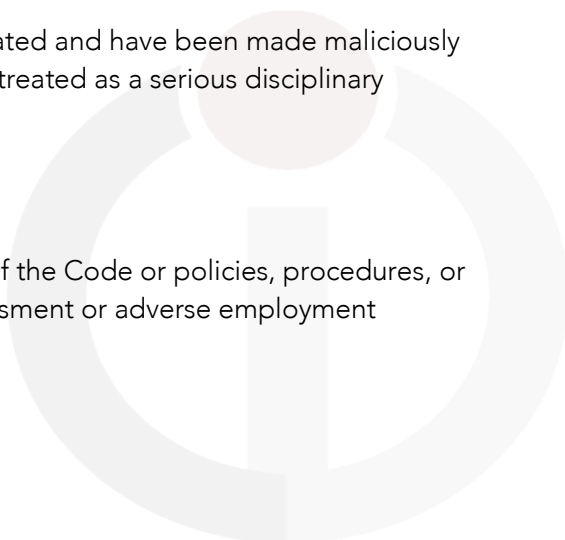
Anyone filing a complaint concerning a violation or suspected violation must be acting in good faith and have reasonable grounds for believing the information disclosed indicates a violation of the Code, policies, procedures or law.

Any good faith report, concern or complaint is fully protected by this policy, even if the report, question or concern is not substantiated after investigation.

Any allegations that prove not to be substantiated and have been made maliciously or with knowledge that they were false will be treated as a serious disciplinary offense.

D. No Retaliation

Anyone who in good faith reports a violation of the Code or policies, procedures, or law shall not be retaliated upon or suffer harassment or adverse employment



consequence. His or her identity will be protected by the Whistleblowing coordinator.

E. The Escalation Process of Raising Concerns

Officers and Employees, as well as partners, customers, vendors, suppliers and other stakeholders may report orally or in writing any suspected violations of this Code, unethical conduct, fraud, and other malpractices to the whistleblowing coordinator.

The Board of Trustees has given a commitment to handle such reports with strict confidentiality and discretion and protect the identity of the person making such a report. Such persons shall be granted protection from any retaliation that may come from the parties being reported. For that reason, the identity will only be known to Whistleblowing coordinator (unless there are overarching reasons to deviate from this policy).

F. Confidentiality

Management will use its best efforts to protect the confidentiality of the complainant for any good faith report. Reports of violations or suspected violations will be kept confidential to the extent possible, consistent with the need to conduct an adequate investigation.

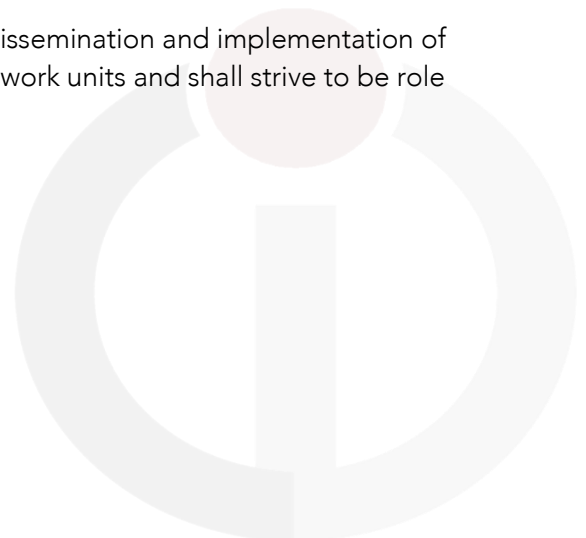
Concerns raised anonymously shall not be entertained.

G. Handling of Reported Violations

The ICD President shall be accountable for the publication of this Code and shall ensure that all Officers, and Employees receive a copy thereof.

For reports on violations, the Whistleblowing Coordinator shall ensure a confidential investigation is immediately undertaken to determine the veracity of the report, gather pertinent data, and recommend appropriate sanctions such as issuance of letter of caution/warning/reprimand or suspension. Violations may lead to separation from the service of ICD and may include reporting to the Authorities and filing of legal suits on behalf of the INSTITUTE.

All Managers are responsible for the proper dissemination and implementation of the provisions of this Code in their respective work units and shall strive to be role models of the Code's provisions.



This Code and other relevant rules and regulations, shall serve as guide in determining the penalties and sanctions to be imposed where violations are proven and validated in accordance with the provisions of **Annex F** hereof.

The principle of due process shall be observed in the handling of all cases.

The Audit and Risk Oversight Committee shall be informed of all such complaints or reports and their status to be rendered by the Compliance Officer.

—oOo—



INSTITUTE OF CORPORATE DIRECTORS, INC.

DATA PRIVACY POLICY

I. DEFINITIONS

Data Privacy Act or **DPA** refers to the Republic Act No. 10173 or the Data Privacy Act of 2012 and its implementing rules and regulations

Data Subject refers to an individual whose Personal Information, Sensitive Personal Information, or Privileged Information is processed.

Organization refers to INSTITUTE OF CORPORATE DIRECTORS, INC.

Personal Data collectively refers to Personal Information, Sensitive Personal Information, and Privileged Information, as defined herein.

Personal Information refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

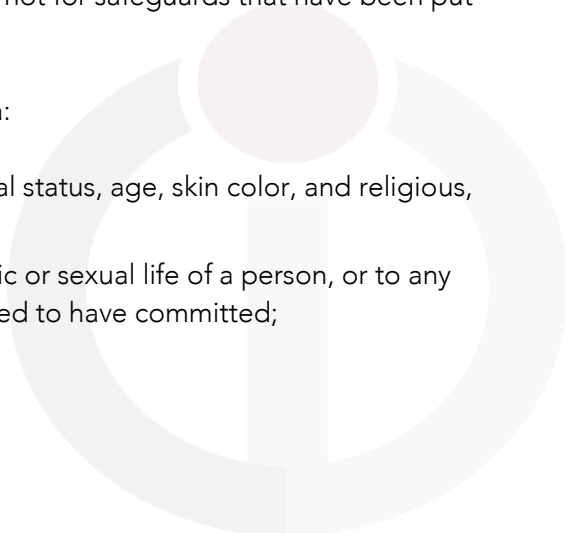
Processing refers to any operation or set of operations performed upon Personal Data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the Personal Data are contained or are intended to be contained in a filing system.

Privileged Information refers to any and all forms of Personal Data, which, under the Rules of Court and other pertinent laws constitute privileged communication.

Security Incident is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of Personal Data. It includes incidents that would result to personal data breach, if not for safeguards that have been put in place.

Sensitive Personal Information refers to Personal Data:

- (a) About an individual's race, ethnic origin, marital status, age, skin color, and religious, philosophical or political affiliations;
- (b) About an individual's health, education, genetic or sexual life of a person, or to any proceeding or any offense committed or alleged to have committed;



- (c) Issued by government agencies “peculiar” (unique) to an individual, such as social security number;
- (d) Marked as classified by executive order or act of Congress.

II. ORGANIZATIONAL SECURITY MEASURES

a. Data Protection Officer (DPO)

The DPO is responsible for ensuring the Organization’s compliance with applicable laws and regulations for the protection of data privacy and security. The functions and responsibilities of the DPO shall particularly include, among others:

1. Monitoring the Organization’s Personal Data Processing activities in order to ensure compliance with applicable Personal Data privacy laws and regulation;
2. Acting as liaison between the Organization and the regulatory and accrediting bodies, and is in charge of the applicable registration, notification, and reportorial requirements mandated by the Data Privacy Act, as well any other applicable data privacy laws and regulations;
3. Developing, establishing, and reviewing policies and procedures for the exercise by Data Subjects of their rights under the Data Privacy Act and other applicable laws and regulations on Personal Data privacy;
4. Acting as the primary point of contact whom Data Subject may coordinate and consult with for all concerns relating to their Personal Data;
5. Formulating capacity building, orientation, and training programs for employees, agents or representatives of the Organization regarding Personal Data privacy and security policies;
6. Preparing and filing the annual report of the summary of documented security incidents and Personal Data breaches, if any, as required under the Data Privacy Act, and of compliance with other requirements that may be provided in other issuances of the National Privacy Commission.

A. Data Privacy Principles

All Processing of Personal Data within the Organization should be conducted in compliance with the following data privacy principles as espoused in the Data Privacy Act:

1. Transparency. The Data Subject must be aware of the nature, purpose, and extent of the Processing of his or her Personal Data by the Organization, including the risks and safeguards involved, the identity of persons and entities involved in processing his or her Personal Data, his or her rights as a Data

Subject, and how these can be exercised. Any information and communication relating to the Processing of Personal Data should be easy to access and understand, using clear and plain language.

2. Legitimate Purpose. The Processing of Personal Data by the Organization shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.
3. Proportionality. The Processing of Personal Data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal Data shall be processed by the Organization only if the purpose of the Processing could not reasonably be fulfilled by other means.

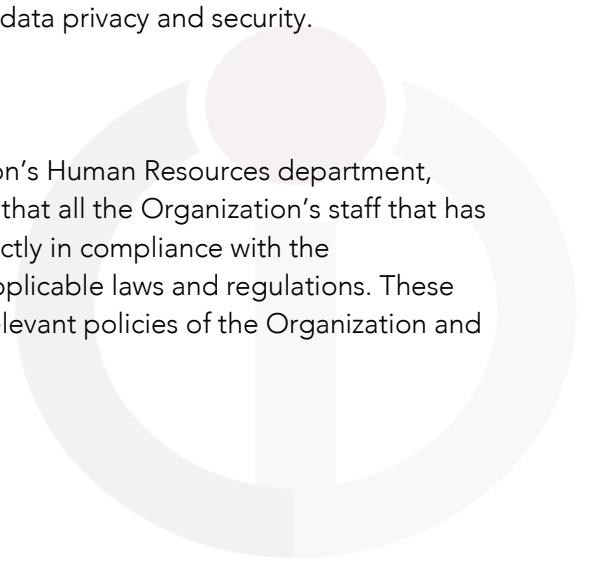
B. Data Processing Records

Adequate records of the Organization's Personal Data Processing activities shall be maintained at all times. The DPO, with the cooperation and assistance of all the concerned business and service units involved in the Processing of Personal Data, shall be responsible for ensuring that these records are kept up-to-date. These records shall include, at the minimum:

1. Information about the purpose of the Processing of Personal Data, including any intended future Processing or data sharing;
2. A description of all categories of Data Subjects, Personal Data, and recipients of such Personal Data that will be involved in the Processing;
3. General information about the data flow within the Organization, from the time of collection and retention, including the time limits for disposal or erasure of Personal Data;
4. A general description of the organizational, physical, and technical security measures in place within the Organization; and
5. The name and contact details of the DPO, Personal Data processors, as well as any other staff members accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

C. Management of Human Resources

The DPO, with the cooperation of the Organization's Human Resources department, shall develop and implement measures to ensure that all the Organization's staff that has access to Personal Data will process such data strictly in compliance with the requirements of the Data Privacy Act and other applicable laws and regulations. These measures may include drafting new or updated relevant policies of the Organization and



conducting training programs to educate employees and agents on data privacy related concerns.

The DPO, with the assistance of HR, shall ensure that Organization shall obtain the employee's informed consent, evidenced by written, electronic or recorded means, to:

1. The Processing of his or her Personal Data, for purposes of maintaining the Organization's records; and
2. A continuing obligation of confidentiality on the employee's part in connection with the Personal Data that he or she may encounter during the period of employment with the Organization. This obligation shall apply even after the employee has left the Organization for whatever reasons.

D. Data Collection Procedures

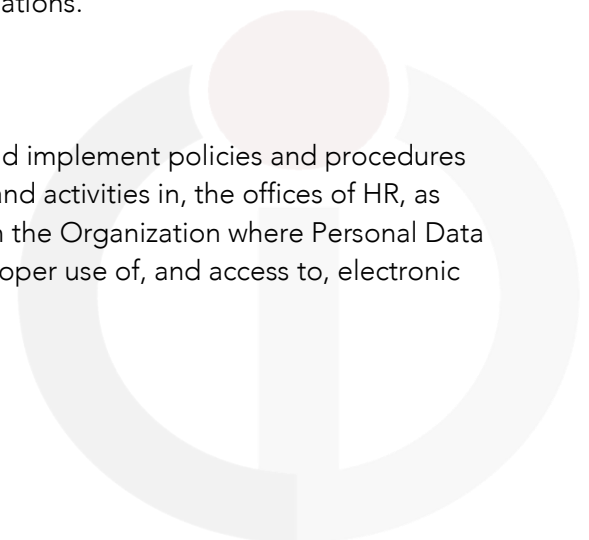
The DPO, with the assistance of the Organization's HR and any other departments of the Organization responsible for the Processing of Personal Data, shall document the Organization's Personal Data Processing procedures. The DPO shall ensure that such procedures are updated and that the consent of the Data Subjects (when required by the DPA or other applicable laws or regulations) is properly obtained and evidenced by written, electronic or recorded means. Such procedures shall also be regularly monitored, modified, and updated to ensure that the rights of the Data Subjects are respected, and that Processing thereof is done fully in accordance with the DPA and other applicable laws and regulations.

E. Data Retention Schedule

Subject to applicable requirements of the DPA and other relevant laws and regulations, Personal Data shall not be retained by the Organization for a period longer than necessary and/or proportionate to the purposes for which such data was collected. The DPO, with the assistance of the Organization's HR and any other departments of the Organization responsible for the Processing of Personal Data, shall be responsible for developing measures to determine the applicable data retention schedules, and procedures to allow for the withdrawal of previously given consent of the Data Subjects well as to safeguard the destruction and disposal of such Personal Data in accordance with the DPA and other applicable laws and regulations.

III. PHYSICAL SECURITY MEASURES

The DPO, with the assistance of HR, shall develop and implement policies and procedures for the Organization to monitor and limit access to, and activities in, the offices of HR, as well as any other departments and/or workstations in the Organization where Personal Data is processed, including guidelines that specify the proper use of, and access to, electronic media.



The design and layout of the office spaces and work stations of the abovementioned departments, including the physical arrangement of furniture and equipment, shall be periodically evaluated and readjusted in order to provide privacy to anyone Processing Personal Data, taking into consideration the environment and accessibility to unauthorized persons.

The duties, responsibilities, and schedules of individuals involved in the Processing of Personal Data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time. Further, the rooms and workstations used in the Processing of Personal Data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

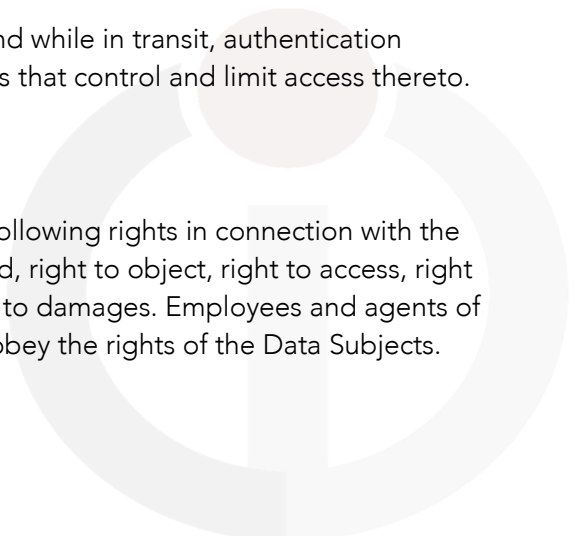
IV. TECHNICAL SECURITY MEASURES

The DPO, with the cooperation and assistance of HR, shall continuously develop and evaluate the Organization's security policy with respect to the Processing of Personal Data. The security policy should include the following minimum requirements:

1. Safeguards to protect the Organization's computer network and systems against accidental, unlawful, or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access;
2. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of the Organization's data processing systems and services;
3. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in the Organization's computer network and system, and for taking preventive, corrective, and mitigating actions against security incidents that can lead to a Personal Data breach;
4. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
5. A process for regularly testing, assessing, and evaluating the effectiveness of security measures; and
6. Encryption of Personal Data during storage and while in transit, authentication process, and other technical security measures that control and limit access thereto.

V. RIGHTS OF THE DATA SUBJECT

As provided under the DPA, Data Subjects have the following rights in connection with the Processing of their Personal Data: right to be informed, right to object, right to access, right to rectification, right to erasure or blocking, and right to damages. Employees and agents of the Organization are required to strictly respect and obey the rights of the Data Subjects.



The DPO, with the assistance of HR shall be responsible for monitoring such compliance and developing the appropriate disciplinary measures and mechanism.

I. Right to Be Informed

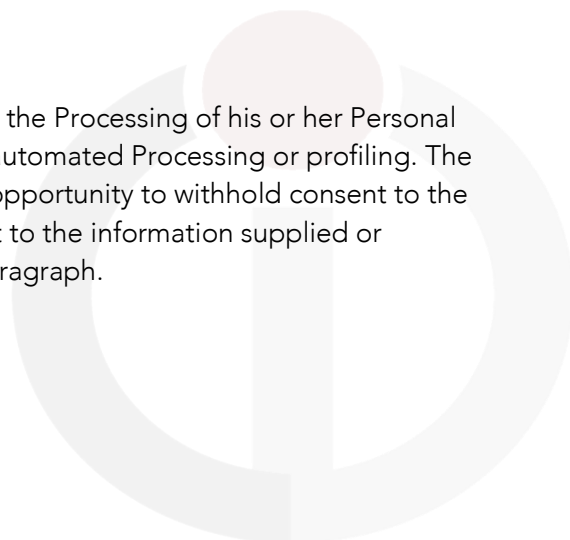
The Data Subject has the right to be informed whether Personal Data pertaining to him or her shall be, are being, or have been processed.

The Data Subject shall be notified and furnished with information indicated hereunder before the entry of his or her Personal Data into the records of the Organization, or at the next practical opportunity:

1. Description of the Personal Data to be entered into the system;
2. Purposes for which they are being or will be processed, including Processing for direct marketing, profiling or historical, statistical or scientific purpose;
3. Basis of Processing, when Processing is not based on the consent of the Data Subject;
4. Scope and method of the Personal Data Processing;
5. The recipients or classes of recipients to whom the Personal Data are or may be disclosed or shared;
6. Methods utilized for automated access, if the same is allowed by the Data Subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject;
7. The identity and contact details of the DPO;
8. The period for which the Personal Data will be stored; and
9. The existence of their rights as Data Subjects, including the right to access, correction, and to object to the Processing, as well as the right to lodge a complaint before the National Privacy Commission.

II. Right to Object

The Data Subject shall have the right to object to the Processing of his or her Personal Data, including Processing for direct marketing, automated Processing or profiling. The Data Subject shall also be notified and given an opportunity to withhold consent to the Processing in case of changes or any amendment to the information supplied or declared to the Data Subject in the preceding paragraph.



When a Data Subject objects or withholds consent, the Organization shall no longer process the Personal Data, unless:

1. The Personal Data is needed pursuant to a subpoena;
2. The Processing is for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the Data Subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the Organization and the Data Subject; or
3. The Personal Data is being collected and processed to comply with a legal obligation.

III. Right to Access

The Data Subject has the right to reasonable access to, upon demand, the following:

1. Contents of his or her Personal Data that were processed;
2. Sources from which Personal Data were obtained;
3. Names and addresses of recipients of the Personal Data;
4. Manner by which his or her Personal Data were processed;
5. Reasons for the disclosure of the Personal Data to recipients, if any;
6. Information on automated processes where the Personal Data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the Data Subject;
7. Date when Personal Data concerning the Data Subject were last accessed and modified; and
8. The designation, name or identity, and address of the DPO.

IV. Right to Rectification

The Data Subject has the right to dispute the inaccuracy or rectify the error in his or her Personal Data, and the Organization shall correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the Personal Data has been corrected, the Organization shall ensure the accessibility of both the new and the retracted Personal Data and the simultaneous receipt of the new and the retracted Personal Data by the intended recipients thereof: Provided, That recipients or third parties who have previously received such processed Personal Data shall be informed of its inaccuracy and its rectification, upon reasonable request of the Data Subject.

V. Right to Erasure or Blocking

The Data Subject shall have the right to suspend, withdraw, or order the blocking, removal, or destruction of his or her Personal Data from the Organization's filing system.

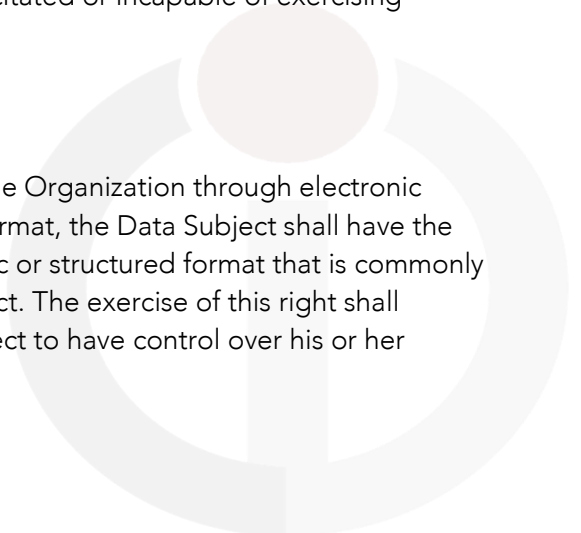
1. This right may be exercised upon discovery and substantial proof of any of the following:
 - (a) the Personal Data is incomplete, outdated, false, or unlawfully obtained;
 - (b) the Personal Data is being used for purpose not authorized by the Data Subject;
 - (c) the Personal Data is no longer necessary for the purposes for which they were collected;
 - (d) the Data Subject withdraws consent or objects to the Processing, and there is no other legal ground or overriding legitimate interest for the Processing by the Organization;
 - (e) the Personal Data concerns private information that is prejudicial to Data Subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
 - (f) the Processing is unlawful; or
 - (g) the Data Subject's rights have been violated.
2. The DPO may notify third parties who have previously received such processed Personal Data that the Data Subject has withdrawn his or her consent to the Processing thereof upon reasonable request by the Data Subject.

VI. Transmissibility of Rights of Data Subjects

The lawful heirs and assigns of the Data Subject may invoke the rights of the Data Subject to which he or she is an heir or an assignee, at any time after the death of the Data Subject, or when the Data Subject is incapacitated or incapable of exercising his/her rights.

VII. Data Portability

Where his or her Personal Data is processed by the Organization through electronic means and in a structured and commonly used format, the Data Subject shall have the right to obtain a copy of such data in an electronic or structured format that is commonly used and allows for further use by the Data Subject. The exercise of this right shall primarily take into account the right of Data Subject to have control over his or her



Personal Data being processed based on consent or contract, for commercial purpose, or through automated means. The DPO shall regularly monitor and implement the National Privacy Commission's issuances specifying the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

VI. DATA BREACHES & SECURITY

a. INCIDENTS DATA MONITORING

1. The DPO, with the assistance of the HR, shall encourage the employees to be responsible in handling Sensitive Personal Information related to the data provided by our partners, members and clients.
2. Adequate records of the Organization's Personal Data Processing activities shall be maintained at all times.
3. The DPO, with the cooperation and assistance of all the concerned departments and service units involved in the Processing of Personal Data, shall be responsible for ensuring that these records are kept up-to-date and secured.
4. All concerned departments shall ensure that the data they receive is processed for specific and legitimate purposes that are proportionate and necessary.
5. The organization should take all necessary measures to protect the data against unauthorized access and ensure that the employees handling the data are sufficiently aware of data protection obligations.
6. In case of breach, follow the guidelines provided to report the Data Breach to the proper authorities.

b. DATA BREACH NOTIFICATION

1. Under Republic Act No. 10173 or the Data Privacy Act of 2012, ICD may be liable to significant fines and penalties if we neglect the reporting for the Data Breach.
2. If there is a detected breach of privacy the employee that detected the breach shall immediately report the facts and circumstances to the Data Protection Officer within 24 hours from his/her discovery.
3. The DPO must verify as to whether or not a breach requiring notification under the Data Privacy Act has occurred as well as for the determination of the relevant circumstances surrounding the reported breach and/or Security Incident.
4. The DPO must also notify the Data Subject immediately after the reported breach on his/her personal data.

5. The DPO shall notify the National Privacy Commission and the affected Data Subjects pursuant to requirements and procedures prescribed by the DPA.
6. The notification to the National Privacy Commission and the affected Data Subjects shall at least describe the nature of the breach, the Personal Data possibly involved, and the measures taken by the Organization to address the breach.

c. DATA BREACH REPORTS

1. All Security Incidents and Personal Data breaches shall be documented through written reports, including those not covered by the notification requirements.
2. In the case of Personal Data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the Organization. In other security incidents not involving Personal Data, a report containing aggregated data shall constitute sufficient documentation.
3. These reports shall be made available when requested by the National Privacy Commission. A general summary of the reports shall be submitted by the DPO to the National Privacy Commission annually.

VII. OUTSOURCING AND SUBCONTRACTING AGREEMENTS

Any Personal Data Processing conducted by an external agent or entity (third-party service provider) on behalf of the Organization should be evidenced by a valid written contract with the Organization. Such contract should expressly set out the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects, the obligations and rights of the Organization, and the geographic location of the Processing under the contract.

The fact that the Organization entered into such contract or arrangement does not give the said external agent or entity the authority to subcontract to another entity the whole or part of the subject matter of said contract or arrangement, unless expressly stipulated in writing in the same contract or evidenced by a separate written consent/agreement of the Organization. The subcontracting agreement must also comply with the standards/criteria prescribed by the immediately preceding paragraph.

In addition, the contract and the subcontracting contract shall include express stipulations requiring the external agent or entity (including the subcontractor) to:

1. Process the Personal Data only upon the documented instructions of the Organization, including transfers of Personal Data to another country or an international organization, unless such transfer is required by law;

2. Ensure that an obligation of confidentiality is imposed on persons and employees authorized by the external agent/entity and subcontractor to process the Personal Data;
3. Implement appropriate security measures;
4. Complies with the Data Privacy Act and other issuances of the National Privacy Commission, and other applicable laws, in addition to the obligations provided in the contract or other legal act with the external party;
5. Not engage another processor without prior instruction from the Organization: Provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the Processing;
6. Assist the Organization, by appropriate technical and organizational measures, and to the extent possible, fulfill the obligation to respond to requests by Data Subjects relative to the exercise of their rights;
7. Assist the Organization in ensuring compliance with the Data Privacy Act and other issuances of the National Privacy Commission, considering the nature of Processing and the information available to the external party who acts as a Personal Information Processor as defined under the Data Privacy Act;
8. At the choice of the Organization, delete or return all Personal Data to it after the end of the provision of services relating to the Processing: Provided, that this includes deleting existing copies unless storage is authorized by the Data Privacy Act or other applicable laws or regulations make available to the Organization all information necessary to demonstrate compliance with the obligations laid down in the Data Privacy Act, and allow for and contribute to audits, including inspections, conducted by the Organization or another auditor mandated by the latter; and
9. Immediately informs the Organization if, in its opinion, an instruction violates the Data Privacy Act or any other issuance of the National Privacy Commission.

—oOo—



INSTITUTE OF CORPORATE DIRECTORS, INC.

POLICY ON RELATED PARTY TRANSACTIONS

I. DEFINITION OF RELATED PARTIES

“**Related Parties**” shall mean the INSTITUTE OF CORPORATE DIRECTORS, INC. and its controlling Fellows and other Members, co-venturers, associates, affiliates, Officers and Trustees, including their spouses, children and dependent siblings and parents, and that of interlocking director relationships by members of the Board.

Parties are considered to be related to the INSTITUTE if there is the ability, directly or indirectly, to control the INSTITUTE or exercise significant influence over the INSTITUTE in making financial and operating decisions, or vice versa, or where the INSTITUTE and the party are subject to common control or common significant influence.

II. COVERAGE AND MATERIALITY THRESHOLD

This Policy on Related Party Transactions (“RPT Policy”) shall cover the following material RPTs only:

- (a) Mergers and acquisitions between Related Parties;
- (b) Loans or advances to and from a Related Party exceeding Philippine Pesos One Million (Php1,000,000.00) per transaction or series of transactions, provided that loans or advances to and from individual directors, including their spouses, children and dependent siblings and parents, at whatever amount, which shall be conducted at arm’s length and at market rate, shall be covered by this Policy;
- (c) Engagement of services of a Related Party outside of the ordinary course of business with fees exceeding Philippine Pesos One Million (Php1,000,000.00) per engagement or series of engagements, provided that engagement of services of individual directors, including their spouses, children and dependent siblings and parents, at whatever amount, which shall be conducted at arm’s length and at market rate, shall be covered by this Policy.

For purposes hereof, any RPT not expressly provided herein shall not be covered by this RPT Policy and therefore shall not be subject of the Audit Committee (“Committee”) review.

For the avoidance of doubt, the following transactions are expressly excluded from this RPT Policy and therefore shall not be subject of the Committee review:

- (a) Compensation of directors and employment of Executive Officers;

- (b) Transactions with similar terms available to all employees generally;
- (c) Banking, treasury and foreign exchange transactions, finance or insurance-related services and transactions with a Related Party, if the terms are generally the same as or similar to offers of other banks or insurance companies in the ordinary course of business;
- (d) Transfer of resources between INSTITUTE and its affiliates.

III. GUIDELINES TO ENSURE ARM'S LENGTH TERMS

RPTs shall be accounted for at market prices normally charged to unaffiliated customers or parties for similar goods, services or transaction.

In the review of the RPTs, the Committee shall consider the following factors:

- (a) The terms of the transaction;
- (b) The aggregate value of the transaction;
- (c) Whether the terms of the transaction are no less favorable than those generally available to non-related parties under the same or similar circumstances;
- (d) The extent of Related Party's interest in the transaction;
- (e) Purpose and timing of the transaction;
- (f) Whether the transaction would present an improper conflict of interests or special risks or contingencies for the INSTITUTE or any of its affiliates, or the Related Party taking into account the size of the transaction and the overall financial position of the Related Party; and
- (g) Any material information or other factors that the Committee deems relevant.

IV. IDENTIFICATION AND PREVENTION OR MANAGEMENT OF POTENTIAL OR ACTUAL CONFLICTS OF INTEREST

The identification, prevention and management of any conflict of interest are covered by the INSTITUTE's Policy on Conflict of Interest and the Code of Business Conduct and Ethics.

One way to identify, prevent or manage potential or actual conflict of interest as stated in our Code of Conduct and Policy on Conflict of Interest is the obligation of every Trustee, Officer and Employee, to declare and divulge in writing to the INSTITUTE his/her own involvement in any conflict of interest with the INSTITUTE. A Related Party Disclosure Form is accomplished and submitted on an annual basis.

V. REVIEW BY THE AUDIT COMMITTEE

The Committee shall review and approve all covered RPTs as provided in Section II above in accordance with the principles of transparency, integrity and fairness, to ensure that they are at arm's length, the terms are fair, and they will inure to the best interest of the Corporation and its subsidiaries or affiliates and their shareholders, including minority shareholders.

If a transaction passes the review of the Committee, the Committee shall endorse the same to the Board of Directors for final approval.

Any member of the Committee or Board of Trustees who has an interest in the RPT under review shall immediately inform the Committee of the circumstance and abstain from participating in the discussion and from voting thereon. However, the presence of such member may be counted in determining the presence of a quorum at the meeting of the Committee or Board of Trustees.

VI. WHISTLEBLOWING MECHANISM

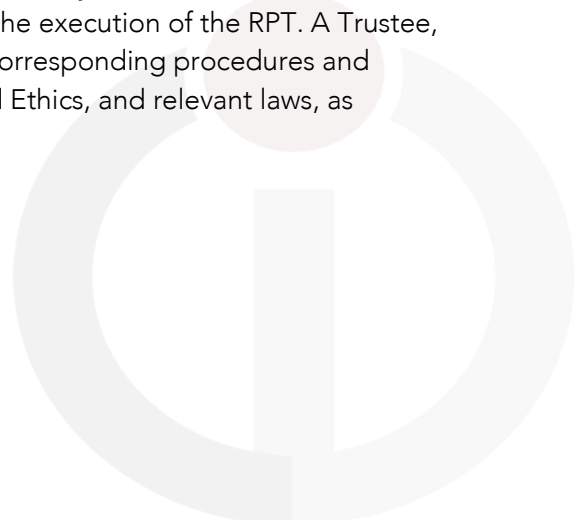
The Whistleblowing Policy as stated in the Code of Business Conduct and Ethics shall apply to any abuse of RPT. Whistleblowing in relation to RPTs shall be reported to the Whistleblowing coordinator.

In addition to whistleblowing made available to all stakeholder, they are provided with proper guidelines and procedures for right of action and remedies that are readily accessible in order to redress the conduct of the company (e.g. Facebook page, Twitter account, E-mail account, and Hotline numbers), as necessary.

VII. RESTITUTION OF LOSSES AND OTHER REMEDIES FOR ABUSIVE RPTS

Rights of Fellows and other members are protected at all times, especially from abusive actions by, or in the interest of controlling Fellows and Trustees. ICD ensures that its policies and processes cater to the best interest of all its Fellows and other members, and other stakeholders. As such, all transactions including RPTs that require Fellows' approval, as determined by the Committee, are submitted to all Fellows, for approval. The INSTITUTE shall encourage disinterested shareholders to decide on the matter.

Non-compliance with any of the provisions of this RPT Policy shall result in the nullification or revocation of any agreement or contract involved in the execution of the RPT. A Trustee, Officer, Employee or Related Party is subject to the corresponding procedures and penalties under ICD's Code of Business Conduct and Ethics, and relevant laws, as applicable.



VIII. DISCLOSURE OF RPTS

RPTs are disclosed in the INSTITUTE's financial statements, annual reports, and other applicable filings in accordance with the relevant rules and issuance of the Securities and Exchange Commission (SEC), and other applicable regulatory bodies.

The disclosure includes, but is not limited to, the name of the related party, relationship with the company for each RPT, the nature, and value for each RPT.

Such disclosure is also made publicly-available by the company, for the benefit of all shareholders and other stakeholders, through the company website and such other media channels as applicable.

—oOo—



INSTITUTE OF CORPORATE DIRECTORS, INC.

POLICY AND PROCEDURES IN CONFLICT OF INTEREST SITUATIONS**A. POLICY**

All Officers and Employees of the INSTITUTE shall avoid conflict of interest situations. Any potential or actual conflict of interest situation shall be disclosed immediately to allow Management to assess risks related to the situation and provide appropriate safeguards, when necessary, to ensure fairness and integrity of ICD's transactions.

All Officers and Employees are required to disclose any financial or personal interest or benefit in any transaction involving ICD to ensure that potential conflicts of interest are immediately brought to the attention of Management.

Even the appearance of impropriety and the potential for conflict should be disclosed and avoided.

1. Conflict of Interest

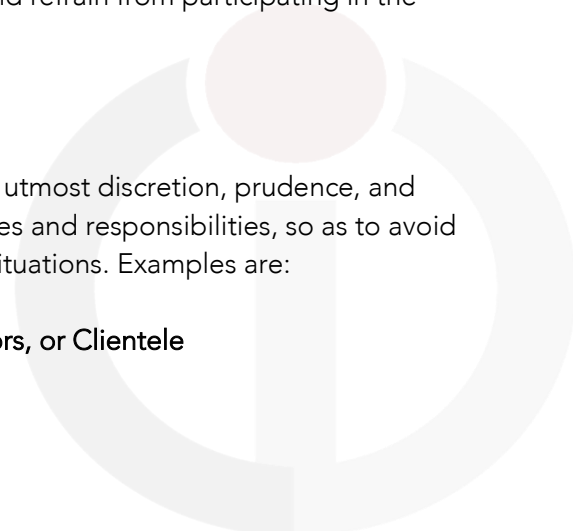
Conflict of interest refers to any situation in which an individual with responsibilities to others might be, consciously or unconsciously, influenced by financial, or other factors that involve self-interest.

A conflict of interest situation is present where a person has a private or personal interest, sufficient to appear to influence the objective exercise of his/her official duties. In other words, conflict of interest exists when there is personal benefit and/or bias involved in decision-making. The personal benefit or bias may be real or perceived.

If a reasonable, disinterested person would conclude that an individual might prioritize personal interests over his responsibilities to ICD, there is, at the very least, the appearance of a conflict of interest. Whether real or perceived, the conflict of interest must be disclosed forthwith and the person should refrain from participating in the decision process.

2. Factors Driving Conflict of Interest

Each Officer or Employee is enjoined to exercise utmost discretion, prudence, and mature judgment in the discharge of his/her duties and responsibilities, so as to avoid both appearance and actual conflict-of-interest situations. Examples are:

(a) Interest in Businesses of Suppliers, Competitors, or Clientele

This refers to any financial interest in the business of a supplier, competitor or client of ICD. Financial interest or management participation by an immediate family member needs to be disclosed as well;

(b) Employment or Analogous Service in the Business of a Supplier, Contractor or Clientele

Engagement by such entities as a Director, adviser, Officer, employee or consultant needs to be disclosed and requires approval by ICD, through its President. Engagement in such capacity of an immediate member of the family (parent, brother, sister, spouse, child) needs to be disclosed as well;

(c) Engagement by Other Commercial Enterprises or in a Political Office

Engagement in another occupation or provision of service to any other commercial enterprise, as well as holding of a concurrent position in government in addition to one's position in ICD needs to be disclosed and requires approval by ICD;

(d) Acceptance of Gifts and Entertainment

Gifts, entertainment and travel of significant value may not be accepted from any supplier or customer of ICD. Neither may an immediate family member or representative accept such on behalf of the Trustee, Officer or Employee.

See Annex D on **Guidelines on Acceptance of Gifts** and Annex E on **Guidelines on Travel Sponsored by Business Partners**.

(e) Political Activities

Active involvement in any political party or political campaign should be disclosed and requires permission from ICD.

(f) Relatives in the Same Company

Disclosure should be made when an employee has a relative who is employed in the INSTITUTE. The same is true when applicants for a position have relatives working in ICD. Management may exercise its discretion on such disclosure ICD does not allow possible situations where there will be relatives with a superior-subordinate relationship or in a control function exercised over the department of a relative.

In addition to the presence of relatives in such situations, employees should disclose any personal relationship when such begins to exist with another employee where one exercises a superior-subordinate relationship or control relationship with the employee.

3. Reporting Requirements

All Officers and Employees are required to voluntarily disclose to the ICD President real or potential conflicts as they arise or at every January of each year.

The Procedures and Review in conflict of interest situations are provided for in Annex 1 (below).

B. PROCEDURE

1. Duty to Disclose

Every Trustee, Officer and Employee of ICD shall disclose to the Approving Authority all material facts regarding his/her interest in the transaction, promptly upon learning of the proposed transaction.

2. Determining Whether a Conflict of Interest Exists

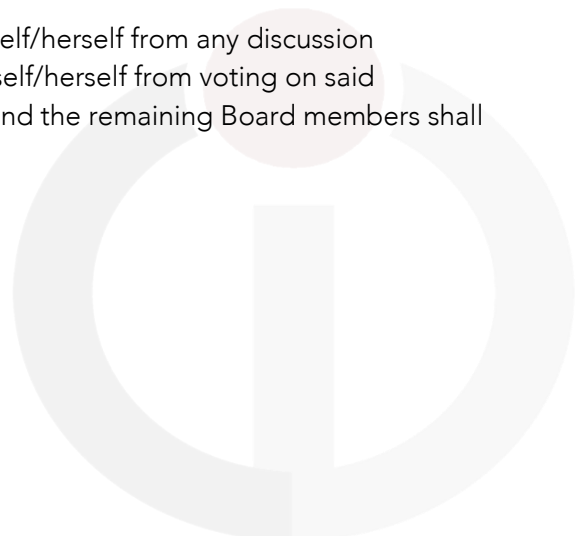
(a) **"Approving Authority"** – The President/CEO shall be deemed the approving authority in the case of Officers and Employees and consultants of ICD. The ICD Board of Trustees shall be deemed the approving authority insofar as the President/CEO or any Trustee.

(b) With regard to an interested Officer or Employee, the Approving Authority shall determine if a conflict of interest exists. The interested Officer or Employee shall not be present during the Approving Authority's discussion or determination of whether a conflict of interest exists except as provided in Section B below on Review of Transactions.

3. Procedures for Addressing a Conflict of Interest

The Approving Authority shall follow the procedures set forth in Section B below in order to decide what measures are needed to protect ICD's interests in light of the nature and seriousness of the conflict, to decide whether to enter into the transaction and, if so, to ensure that the terms of the transaction are appropriate.

In the case of a Trustee, he/she shall excuse himself/herself from any discussion involving the transaction and likewise inhibit himself/herself from voting on said transaction in which the Trustee has an interest, and the remaining Board members shall decide the matter.



C. REVIEW OF TRANSACTIONS

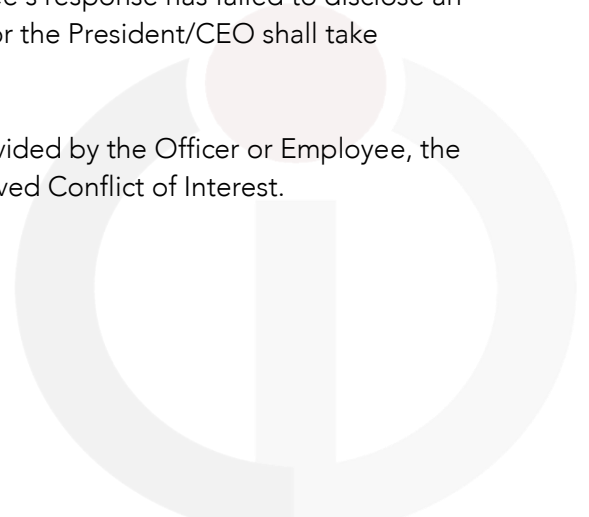
1. The Approving Authority may ask questions of and receive presentations from the potentially conflicted Officer or Employee and any other interested persons and may deliberate and vote on the transaction in their presence.
2. The Approving Authority shall ascertain that all material facts regarding the transaction and the interested person's conflict of interest have been disclosed to it and shall compile appropriate data to ascertain whether the proposed transaction is just and reasonable to the INSTITUTE.
3. After exercising due diligence, which may include investigating alternatives that present no conflict, the Approving Authority shall determine whether the transaction is in the INSTITUTE's best interest, for its own benefit, and whether it is just and reasonable to the INSTITUTE; the transaction can be approved by the Approving Authority (ICD authorization and approval matrix).

D. ANNUAL DISCLOSURE AND COMPLIANCE STATEMENTS

1. ICD Officers and Employees shall annually sign a statement on the form attached (Annex 1-A), that:
 - (a) Affirms that the person has received a copy of this conflict of interest policy, has read and understood the policy, and has agreed to comply with the policy; and
 - (b) Discloses the person's financial interests and family relationships that could give rise to conflicts of interest.

E. VIOLATIONS

1. If the ICD Board or the President/CEO has reasonable cause to believe that an Officer or Employee has failed to disclose actual or possible conflicts of interest, including those arising from a transaction with a related interested person, it shall inform such individual concerned of the basis for this belief and afford the him/her an opportunity to explain the alleged failure to disclose.
2. If, after hearing the conflicted Officer or Employee's response has failed to disclose an actual or possible conflict of interest, the Board or the President/CEO shall take appropriate disciplinary and corrective action.
3. It is possible that on the basis of information provided by the Officer or Employee, the Board concludes that there was no real or perceived Conflict of Interest.



F. ANNUAL REVIEWS

1. To ensure that the INSTITUTE operates in a manner consistent with its status as a non-stock non-profit organization, the Board shall authorize and oversee an annual review of the administration of this Conflict of Interest policy.
2. The review, which may be written or oral, shall consider the level of compliance with the Policy, the continuing suitability of the policy, and whether the policy should be modified and improved.



**CONFLICT OF INTEREST POLICY:
ACKNOWLEDGMENT AND FINANCIAL INTEREST
DISCLOSURE STATEMENT**

The INSTITUTE OF CORPORATE DIRECTORS follows a conflict of interest policy designed to foster public confidence in our integrity and to protect our interest when we are contemplating entering a transaction or arrangement that might benefit the private interest of a director, a corporate officer, our top management official and top financial official, any of our key employees, or other interested persons. Loyalty, honesty, truthfulness and moral virtue are expected to be practiced and uphold in all action at all times.

I. Acknowledgment of Receipt

I hereby acknowledge that I have received a copy of the conflict of interest policy of **Institute of Corporate Directors, Inc.**, have read and understood it and agree to comply with its terms.

Signature

Date

Printed Name



II. Disclosure of Financial Interests

Part II

Please check ONE of the following boxes:

My interests and relationships have not changed since my last disclosure of interests.

OR

I hereby disclose or update my interests and relationships that could give rise to a conflict of interest: [Complete the table below. Use additional pages as needed.]

Family Relationships	Names of those presenting a potential conflict of interest
Include spouse/domestic partner, living ancestors, brothers and sisters (whether whole or half blood), children (whether natural or adopted), grandchildren, great grandchildren, and spouses/domestic partners of brothers, sisters, children, grandchildren, and great grandchildren	
Type of interest	Description of interest that could lead to a conflict of interest
Transactions or arrangements with the Organization	
Transactions or affiliations with other nonprofit organizations	
Substantial business or investment holdings	
Transactions or affiliations with businesses not listed above	

I am not aware of any financial interest involving me or a family member that could present a conflict of interest that I have not disclosed either above or in a previous disclosure statement.

Signature

Date

Printed Name



INSTITUTE OF CORPORATE DIRECTORS, INC.

GUIDELINES ON ACCEPTANCE OF GIFTS

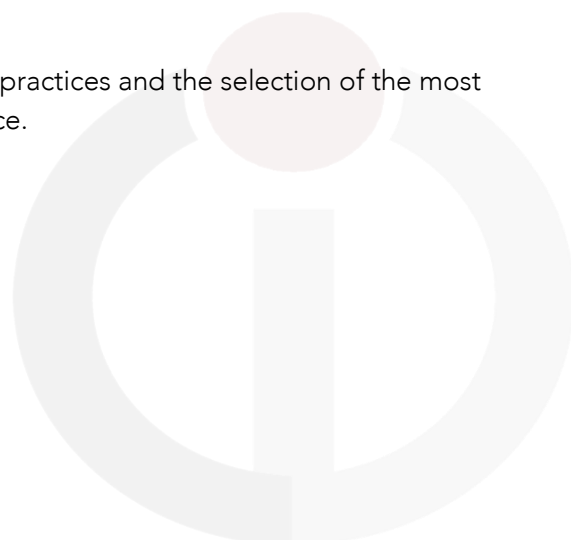
THE INSTITUTE OF CORPORATE DIRECTORS OF THE PHILIPPINES is committed to strengthen its own corporate governance practices in the workplace with the end in view being a living example in pursuing its **MISSION: "To advocate good governance in the corporate sector for the benefit of society."**

In line with this, ICD hereby expressly prohibits the solicitation or acceptance of gifts from business and program partners, suppliers and other vendors. All ICD Trustees, Officers and Employees shall be bound by the following Guidelines:

1. The INSTITUTE prohibits the giving, offering, solicitation or acceptance of gifts in any form from a business or program partner (i.e., contractors, suppliers, banks and other entities engaged in business with ICD), directly or indirectly, by any Trustee, Officer or Employee of ICD.
2. The term "gift" covers anything of value, such as ,but not limited to, cash or cash equivalent, loan, fee, reward, commission, allowance, employment, education, travel, entertainment, sponsorship of personal events (like birthday, wedding, baptism, etc.), the use of property owned by business partners (like vehicles, beach houses, resorts, restaurants, bars, sports or recreational facilities), whether for personal or business use.
3. However, a Trustee, Officer or Employee may accept corporate give-aways, tokens or promotional items of nominal value (pens, mugs, notebooks, and the like), provided that the gift is voluntarily given by a third person without suggestion or solicitation, as a souvenir or out of courtesy, and provided further that the approximate value of the gift does not exceed Two Thousand Pesos. If the approximate value of the gift exceeds PhP2,000.00, it should not be accepted and returned to the giver immediately. The intended recipient will make an internal note of that that is sent to the Audit Committee.
4. In situations where it is deemed improper to refuse a gift, the issue shall be referred to ICD Management for proper disposition.

The policy is intended to ensure integrity in procurement practices and the selection of the most appropriate business and program partner in each instance.

—oOo—



INSTITUTE OF CORPORATE DIRECTORS, INC.

**GUIDELINES ON TRAVEL SPONSORED BY
BUSINESS OF PROGRAM PARTNER**

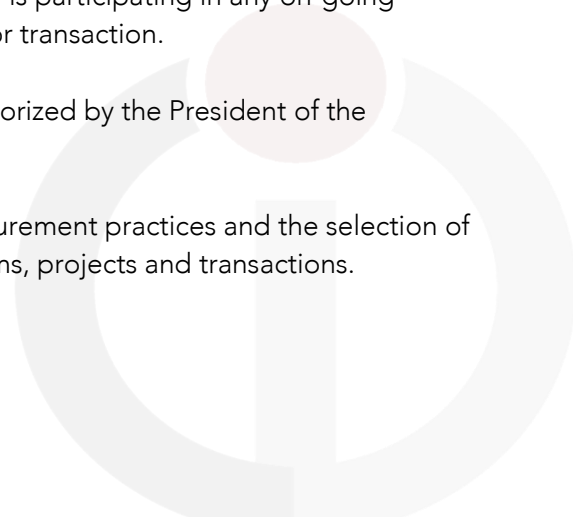
Under the ICD's **GUIDELINES ON ACCEPTANCE OF GIFTS**, all Trustees, Officers and Employees are prohibited from accepting gifts in any form valued more than P2,000 from business or program partners. The term "gift" covers anything of value and includes travel that is sponsored by business partners. The term "business or program partners" refers to advocacy groups, multilateral entities, contractors, suppliers, banks and other entities engaged in business with ICD.

These guidelines are being issued to clarify the prohibition on travel sponsored by business partners.

1. Travel sponsored by a business or a program partner is prohibited, unless it is connected with fulfilling one's duties and responsibilities in a particular ICD project or event. Where a business partner invites ICD Officers or Employees to travel for the purpose of attending trade shows or exhibits where the business partners' products will be featured, or for exposure to new techniques, products and innovations, among similar purposes, Officers and Employees are prohibited from accepting such sponsored travel. If ICD Management deems that such travel is necessary for the business and for the development and training of Officers and Employees, the INSTITUTE will pay for the cost of the travel.
2. Where a project or transaction has been awarded to a business partner and ICD Officers or Employees travel at the expense of ICD to inspect the business partners' project or product not found in Metro Manila or the Philippines to determine its quality, condition or design, such travel shall not be deemed as travel sponsored by a business partners as it is ICD that shoulders the cost for this travel.
3. In no case shall any ICD Officer or Employee accept any travel sponsored by any current or prospective business or program partner which is participating in any on-going bidding or selection process for any ICD project or transaction.
4. Any exception from the foregoing should be authorized by the President of the INSTITUTE.

These guidelines are intended to ensure integrity in procurement practices and the selection of the most appropriate business partner for all ICD programs, projects and transactions.

—oOo—



INSTITUTE OF CORPORATE DIRECTORS, INC.
**DISCIPLINARY PROCEDURES AND PENALTIES FOR VIOLATIONS
OF THE CODE OF BUSINESS CONDUCT AND ETHICS**

A. OBJECTIVE & PURPOSE

1. ICD's policies and procedures are meant to enhance productivity and maintain professionalism in the workplace. Any violation of these policies and procedures or performance of prohibited acts is detrimental to the organization and the achievement of its objectives. Appropriate disciplinary action will be imposed on employees who commit infractions against any of these policies and procedures or display any act of wilful misconduct.
2. The enforcement and implementation of disciplinary action to Officers and Employees is meant to instill discipline, transparency and promote harmony in the organization.
3. Officers and Employees accused of infractions will be given due process.

B. GENERAL GUIDELINES

Unless a particular penalty is imposed for a particular violation or infraction in existing rules and regulations of ICD, any infraction by an Officer or Employee against the Code of Business Conduct and Ethic will be subject to the appropriate disciplinary action taken in the following order:

1. First Offense – Oral Warning

A warning that involves a discussion between the superior and employee about his/her unacceptable behaviour. For the record, the superior shall accomplish a memorandum for the employee's 201 file which will document the discussion and its outcome/results/action steps.

2. Second Offense – Notice to Explain/Written Reprimand

In the event that the employee repeats the behaviour, he/she will be asked by the superior to explain the reason for the infraction in writing. If the employee fails to justify his actions, the superior will issue a written reprimand to the employee. Such reprimand will be included in the employee's 201 file.

3. **Suspension** – Depending on the severity of the infraction and/or repeated offenses, the employee may be suspended for 3 days to 1 week. (See attached table of offenses and penalties)

Employees may be suspended for actions that are considered major offenses such as acts which affect the reputation of the organization or those which cause physical, psychological and emotional harm to co-workers. The employee is not entitled to receive salary and benefits during the period of suspension. Suspension may be imposed without prior oral warning or written reprimand depending on the gravity of the offense.

In the year that an employee has been suspended, he or she will not be eligible to participate in the annual profit sharing.

4. **Dismissal** – Dismissal is an involuntary and unconditional separation of the employee from ICD. It is given when the offense committed is of a higher degree than those mentioned in paragraph 3 above or cause irreparable damage to the reputation of ICD and its staff including but are not limited to fraud, stealing or misusing corporate resources, non-declaration of Conflicts of Interest, submitting false claims for reimbursents and/or commission of a crime (See attached table of offenses and penalties).

Dismissal may also be imposed after repeated suspensions.

A dismissed employee is not eligible to participate in the annual profit sharing over the year in which he forced to leave the employment of ICD.

—oOo—



INSTITUTE OF CORPORATE DIRECTORS, INC.

PROCEDURES FOR REPORTING AND INVESTIGATING HARASSMENT

A. PROCEDURES FOR REPORTING AND INVESTIGATING HARASSMENT

1. Concerned Officer or Employee should report any incident of inappropriate behavior or sexual harassment as soon as possible after the occurrence.

Those who believe they have been harassed, regardless of whether the offensive act was committed by a manager, co-worker, vendor, visitor, or client, should promptly notify their immediate supervisor, designated manager, or Human Resources. They, in turn, will notify the Whistleblowing coordinator.

If the immediate supervisor is involved in the incident, the concerned Officer or Employee should report the incident to the Human Resources Department.

ICD takes claims of harassment seriously, no matter how trivial a claim may appear. All complaints of harassment, sexual harassment, or other inappropriate sexual conduct will be promptly, thoroughly and impartially investigated by the INSTITUTE.

2. ICD prohibits retaliation against any Officer or Employee who files or pursues a harassment claim. To the extent possible, all complaints and related information will remain confidential, except to those individuals who need the information to investigate, educate, or act in response to the complaint.
3. All Officers and Employees are expected to cooperate fully with any ongoing investigation regarding harassment incident. Officers or Employees who believe they have been unjustly charged with harassment can defend themselves orally or in writing at any stage of the investigation.
4. To protect the privacy of persons involved, confidentiality will be maintained throughout the investigatory process to the extent practicable and appropriate under the circumstances. Investigations may include interviews with the parties involved, and, where necessary, individuals who may have observed the alleged conduct or who may have relevant knowledge.
5. At the conclusion of a harassment investigation, the complainant and the alleged "harasser" will be informed of the determination. He or she will have the right to respond. Where appropriate, the "harasser" and the "victim" may be offered mediation or counseling through an employee assistance program.

B. PENALTIES FOR VIOLATION OF ANTI-HARASSMENT POLICY

1. If it is determined that inappropriate conduct has occurred, ICD will act promptly to eliminate the offending conduct, and take such action as is appropriate under the circumstances. Such action may range from counseling to termination of employment and may include such other forms of disciplinary action (such as suspension), as the INSTITUTE deems appropriate under the circumstances and in accordance with applicable law.

—oOo—

