**INFORMATION SECURITY POLICY**

*Handling and Storage of Confidential Information*

## 1.0 Background and Purpose

The International Code of Conduct Association's ("ICoCA," or "the Association") Information Security Policy is designed to assure the highest possible level of protection for all Confidential and Sensitive information provided to or collected by the ICoCA regarding its Members and any related third parties. The intent of the policy it to enhance transparency and encourage the disclosure of relevant information by Members within the Association by providing members assurance (a) that Confidential and Sensitive information provided to the Association will not be disclosed outside of the Association, (b) that such information will be used solely for the purposes of Association, and (c) that access to such Confidential and Sensitive information will be strictly limited to those persons who need access to it in order to carry out the basic functions of the Association.

## 2.0 Definitions

Confidential Information: For purposes of this Information Security Policy, "Confidential Information" refers to all information belonging to Members that is not generally in the public domain, the release of which could result in damage to the commercial interest of Members and/or the privacy interests of its officers, employees, or related entities. Confidential Information includes (but is not limited to):

- Non-public financial information about Members
- Non-public information identifying Members' commercial partners
- Non-public information concerning Members' commercial relationships with clients and other business partners (e.g., commercial terms, contract language, employment terms, etc…)
- Personally-identifying information concerning Members' beneficial owners, officers, employees
- Any information covered by Data Privacy Legislation in areas where Members work or do business

## 3.0 Storage and Handling of Confidential and Sensitive Information

### 3.1 Maintaining Membership Application and other Membership Data

In order to minimize the exposure of Confidential Information to any potential data breaches, information provided by Members as part of their initial Membership Application, Registration Statement, and Implementation Plan submissions (collectively, "Membership Application Data) shall be submitted to the Secretariat in paper form or on stand-alone memory storage media (e.g., CD, flash drive, memory stick) only. The Secretariat will not accept or process

Membership Application Data that is transmitted via e-mail, text, or any other non-secure electronic means.

All Membership Application Data and any information subsequently submitted to or collected by the Secretariat for the purpose of managing Membership (collectively, "Membership Data") shall be stored in a secure database (the "Membership Database") housed on a secure, dedicated server. Such server shall not connect to the Internet nor shall it be reachable from the Internet in any way. The physical network shall be separated where possible and at a minimum, a dedicated Industry Grade Highly Secured Firewall and its corresponding Firewall Rules shall block any IP traffic to and from the Internet to the Database Server.

Backup of the Database shall be limited to a local media, properly stored in a safe place and accessible only by ICoCA's Executive Director and Office Manager.

The original media on which Membership Application Data and any subsequent Membership Data is provided to the Association shall be maintained in a secured location at the offices of the ICoCA for a period of three (3) years following receipt. With the exception of the original media and the data stored in the Membership Database, no other copies of Membership Application Data or Membership Data shall be maintained by the Association.

### 3.2 Access to Confidential Information

Access will be granted to a restricted number of IT Staff who will each have to sign an NDA. External IT suppliers will also sign an NDA between the ICoCA and the legal entity providing the services. The list of IT staff with access will be maintained by the Secretariat and made available to any Member upon request.

Secretariat Staff access to the Membership Database shall be limited to the ICoCA Executive Director and Office Manager, and such other person(s) as the Executive Director shall designate – but in no event shall any person be provided access to the Membership Database if that person is not directly employed by the Association.

A dedicated stand-alone computer, with no internet access, shall be used to input information to the Membership Database. Access to that computer shall be limited to persons with access to the Membership Database.

The above data protection provisions shall be revised in due course to include provision for the protection of data that will be gathered in the course of the Certification, Monitoring and Grievance processes that the ICoCA will implement in the future. The Data Security Policy will be revised at the time of development of the procedures for these processes.

### 3.2 Certification Information (To Be Added)

### 3.3 Monitoring Information (To Be Added)

3.4 Grievance Information (To Be Added)

## 4.0 Reporting to ICoCA Board

4.1 Membership Application and Membership Data

In accordance with the Association's Membership Requirements, the Secretariat shall prepare a summary of an Applicant's submission for membership to the Board of Directors for the purpose of facilitating the Board's decision regarding admission of the Applicant as a Member. Except where authorized in advance by the affected Member, the summary shall not contain Confidential or Sensitive Information.

To the extent that Confidential Information is provided to the Board with the consent of the affected Member or Applicant, the Secretariat will do so either in person (i.e., not in writing) or in paper form only and shall ensure that all copies of Confidential Information are returned by Board Members and destroyed following the conclusion of any meeting or other proceeding at which such Confidential Information is discussed.

## 5.0 Non-Disclosure Agreements

No person shall be permitted access to Confidential and/or Sensitive Information unless and until such person (a) has executed a Non-Disclosure Agreement utilizing the form prepared the Secretariat and approved by the Board.