Professional Association of CISOs
theciso.org

Code of Professional Conduct

10/21/2024 V1.01

Introduction

The purpose of this Professional Association of CISOs ("the Association") Code of Professional Conduct ("Code") is to clearly establish core principles of behavior and corresponding standards of ethical conduct, practice, and qualifications for cybersecurity as a profession. This Code applies to all members of the Association.

This Code of Professional Conduct is based on six Principles covering

1. Professional Integrity
2. Standards of Practice
3. Confidentiality
4. Communications
5. Conflict of Interest
6. Enforcement of the Code

Within each Principle are one or more Fundamental Canons identifying the professional and ethical standards with which a member should strive to comply. These are accompanied by practical Rules of Practice, which provide additional explanatory, educational, and advisory material on how the Fundamental Canons can be interpreted and applied.

This Code of Professional Conduct should be applied subject to applicable laws and legal obligations, in a context-sensitive manner, considering both specific organizational settings and circumstances and the potential for adverse consequences. All PAC Members shall comply with the Code. A Member who commits a material violation of the provisions of the Code shall be subject to the Association's counseling and discipline procedures.

A Member may use this Code as guidance for how to comply with their legal obligations, including the obligation to comply with their Employer's policies, in a manner consistent with the Code. This Code also provides guidance for those situations not covered by their Employer's policies.

Laws may also impose obligations upon a Member. Where requirements of Law conflict with the Code, the requirements of Law shall take precedence.

A Member is responsible for being familiar with, and keeping current with, this Code and applicable laws and legal obligations. A Member is accountable for understanding such Laws or rules of conduct as may be necessary and for seeking legal advice as needed.

Code of Professional Conduct

The Fundamental Canons ("Canons") of the Code identify the professional and ethical standards with which a Member shall comply. Canons are grouped by Principle (such as Professional Integrity). Each Principle may have one or more Fundamental Canons. The Rules of Practice, as Annotations, provide additional explanatory, educational, and advisory material on how the Fundamental Canons are to be interpreted and applied. Each Canon may have Rules of Practice for those situations where additional guidance is required.

Professional Integrity

Fundamental Canon 1: Members shall strive to conduct all their relations with honesty and integrity.

Annotation 1.1: A Member shall not engage in any professional conduct involving dishonesty, fraud, deceit, or misrepresentation.

Annotation 1.2: A Member shall not commit any act that, in the determination of the PAC, reflects adversely on the cybersecurity profession.

Annotation 1.3: Members shall not falsify their qualifications or permit misrepresentation of their qualifications or prior assignments.

Fundamental Canon 2: A Member shall strive to conduct themselves with professional courtesy and to treat all persons with dignity, respect, fairness and without discrimination.

Standards of Practice

Fundamental Canon 3: A Member shall ensure that they have the appropriate education and experience to ensure the skills and knowledge for the tasks required for their role, such as laid out by the PAC or other entities as applicable to the Member's role as a cybersecurity professional.

Annotation 3.1: Members shall strive to stay current with standards and advances in cybersecurity.

Annotation 3.2: Regardless of the presence or absence of education or experience standards, a member must ensure that they have the appropriate skills and experience required for their area of responsibility.

Fundamental Canon 4: Members shall consistently, visibly and transparently disclose, to an organization's stakeholders, the organization's current cybersecurity risks, threats and the adequacy of controls for the organization's stated risk tolerance.

Annotation 4.1: Members are responsible for full, fair, accurate, timely and understandable description of risks, and the {adequacy, appropriateness} of the controls for the mitigation of risk.

Annotation 4.2: Members acting in the role of CISO should review the cybersecurity risk statements that are provided to their Employer's executive leadership, customers, regulators as appropriate, for accuracy and completeness and should bring to the attention of the executive leadership team, including as appropriate, the CEO/President, the Board of Directors, those cybersecurity risks and threats that affect the operations and disclosures made by the Company.

Fundamental Canon 5: Recognizing that the exchange of actionable cybersecurity information is essential to furthering cybersecurity collective defenses, Members shall ensure the appropriate sharing of information in compliance with applicable laws and legal obligations.

Annotation 5.1: Members should participate in formal information exchange mechanisms, including international, national, or industry-based information sharing organizations to ensure the timely exchange of information about threats and vulnerabilities, subject to applicable laws and legal obligations.

Annotation 5.2: Recognizing that there may be times where resiliency efforts require an immediate sharing of information, Members should ensure that they have established rules of engagement with their Employer to ensure timely participation in, and aid from, information sharing as part of the response to a cybersecurity threat.

Confidentiality

Fundamental Canon 6: A Member must not disclose to another party any Confidential Information unless explicitly authorized or required by applicable law or legal obligations.

Communications

Fundamental Canon 7: Members shall take appropriate steps to ensure that their cybersecurity communications, whether written, electronic, or oral, are clear and appropriate to the circumstances and its intended audience and shall work to ensure that these communications include all relevant and pertinent information.

Annotation 7.1: Recognizing the risks of misquotation, misinterpretation, or other misuse of communications, Members shall take reasonable steps to include, as appropriate the Member's name and their role, the intended audience for the communication, the date of issuance of the Communication and any markings required to indicate limitations on the distribution and use of communications, and if acting on behalf of an organization, the organization's name.

Annotation 7.2: Recognizing that the statements of cybersecurity maturity and risk posture may change over time as new information becomes available, Members shall take reasonable steps to ensure the review of any external communications (such as presentations, white papers) by an appropriate third party.

Fundamental Canon 8: Members shall avoid the use of communications containing a material misrepresentation of fact, omitting a material fact, or otherwise commenting on a subject without firm evidence.

Annotation 8.1: Members shall not offer statements about emerging, ongoing or past cybersecurity events without evidence, or in the case of the Member's employer, without authorization.

Annotation 8.2: Members shall ensure that their opinions are clearly identified as such and not represented as statements of fact.

Conflict of Interest

Fundamental Canon 9: A Member shall ensure their interests and relationships, including personal or financial, do not have the appearance or potential to interfere with the Member's ability to make impartial decisions in their professional role (a Conflict of Interest), and when such potential exists, it is appropriately disclosed to affected parties.

Annotation 9.1: In the case of an actual or potential Conflict of Interest, the Member shall ensure that the conflict has been disclosed, in compliance this Cod and subject to applicable laws and legal obligations, including employer policies, and otherwise ensuring that:

- There has been disclosure of an actual or probable conflict to affected parties;
- All such affected parties have expressly agreed to the performance of the cybersecurity services by the Member; and
- The agreement has been dated and recorded and is available to the affected parties.

Annotation 9.2: Members shall not accept other employment including but not limited to part time employment, consultancy, and advisory work. to the detriment of their regular work or interest.

Fundamental Canon 10: Members shall not solicit or accept direct or indirect compensation from more than one party, unless the circumstances are fully disclosed and agreed to by all interested parties.

Annotation 10.1: Members who are acting as independent agents, providing services to multiple parties, should ensure and reasonably believe that they will be able to provide competent and diligent representation to each affected client.

Fundamental Canon 11: Members shall be transparent in their actions including the disclosure of activities that may be perceived as exposing the Member to undue or external influence over their decisions or actions, including through the receipt or exchange of Gifts, Meals, Entertainment, Travel, or Future Compensation ("GMETFC").

Annotation 11.1: Members must ensure that GMETFC should be reasonable and appropriate to the business relationship, local laws and customs and the member's Employers' policies.

Enforcement of the Code

Fundamental Canon 12: A Member who believes that they are being asked or required to act in violation of the Code shall confirm and clarify the ask, explain why they believe the ask conflicts with the Code and work to ensure an outcome that is consistent with this Code. If such a discussion is not possible or not successful, the Member may seek an opinion from the Committee of Professional Conduct.

Annotation 12.1: If a Member believes that they may have violated the Code, the Member should seek guidance from the Committee of Professional Conduct of the PAC.

Fundamental Canon 13: A Member with knowledge of an apparent, unresolved, meaningful violation of the Code, shall attempt to resolve the apparent violation through discussion and clarification. If such a discussion is not attempted or is not successful, the member shall disclose the violation to the appropriate counseling of the Association, except where the disclosure would be contrary to law, would divulge Confidential Information.

Fundamental Canon 14: Members shall respond promptly, truthfully, and fully to request for information by, and cooperate fully with, an appropriate counseling and disciplinary body of the Association in connection with any disciplinary, counselling, or

other proceeding of the Association relating to the Code subject to applicable laws and legal obligations.

Fundamental Canon 15: Members shall be open and cooperative with authorized external parties as part of an investigation into potential violations of regulations, this Code, or the Law.

Annotation 15.1 Members may engage independent legal representation in case of an investigation including potential violations of regulations, this Code, or the Law, to ensure fair representation of the Member and their interests.

Effective Date: October 20, 2024