

ICLA

INTERNATIONAL CYBERSECURITY LEADERSHIP ASSOCIATION

CODE OF PROFESSIONAL CONDUCT

Core principles of ethical conduct, practice, and qualifications
for cybersecurity leaders.

CONTENTS

Contents

-
- 01 Introduction**
 - 02 Definitions**
 - 03 Code of Professional Conduct**
 - Professional Integrity
 - Standards of Practice
 - Confidentiality
 - Communications
 - Conflict of Interest
 - Enforcement of the Code
 - 04 Proposed Topic Areas**
 - 05 Version History and Change Log**
 - 06 Contributors**
-

01 / SECTION

Introduction

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

This Code is based on the initial work completed by the authors through the ICLA and released under Creative Commons License.

This Code of Professional Conduct is based on six Principles covering Professional Integrity, Standards of Practice, Confidentiality, Communications, Conflict of Interest, and Enforcement of the Code.

Within each Principle are one or more Fundamental Canons identifying the professional and ethical standards with which a member is expected 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. The Rules of Practice provide guidance on the interpretation of the Canons and may be used to assert and confirm the reasonableness of behavior in compliance with a Canon.

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 ICLA Members shall follow the Code. A Member who commits a material violation of the provisions of the Code shall be subject to the Association's counseling and procedures for review of conduct.

A Member may use this Code as a guide 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.

PROFESSIONAL AND LEGAL COUNSEL

This Code does not prevent a member from seeking professional advice in connection with their duties to clients or employers, or for guidance on personal legal or financial risks. Members may consult with professionals such as attorneys or CPAs for such advice, provided that the professional is bound by a non-disclosure agreement or has a duty of confidentiality to protect the member's confidentiality obligations.

In particular, conversations with attorneys in the United States are protected by attorney-client privilege, allowing you to share confidential information as needed. Members retain the right to seek independent legal or professional counsel without restriction from the organization's internal confidentiality policies.

02 / SECTION

Definitions

As used throughout the Code, the following terms are capitalized and have the meanings indicated:

Chief Information Security Officer An experienced cybersecurity professional who is acting as the head of cybersecurity in an organization, regardless of their actual title. The role of CISO may be filled by an individual with a title that includes Chief Security Officer, Chief Trust Officer, Head of Security, Director - Information Security or similar designation or a non-security related title such as Chief Information Officer. It is the position of the International Cybersecurity Leadership Association that the CISO, as a cybersecurity-focused professional, is responsible for leading an organization's cybersecurity program in compliance with relevant regulations and Laws according to the organization's risk tolerance. The CISO is responsible for understanding the organization's cybersecurity risks and threats, the effectiveness of the technical and organizational controls, and the adequacy of controls in place to manage the organization's risk posture. As the primary cybersecurity liaison to an organization's executive leadership, including the Board of Directors if applicable, and organizational stakeholders, the CISO shall report on the organization's cybersecurity program, the adequacy of controls to manage the cybersecurity risks and threats, and the overall cybersecurity risk posture.

Confidential Information Information is considered confidential if its unauthorized disclosure could harm the organization or provide an adverse impact on its objectives (ISO/IEC 27002:2022). Within an organization this will include information that is of a proprietary nature that is bound by policy, legal, regulatory, or contractual obligations and is protected from being disclosed without authorization.

Conflict of Interest A Conflict of Interest occurs when a person's interests, including personal or financial interests or relationships, have the appearance or potential to interfere with the individual's ability to make decisions objectively, fairly, and in the reasonable interest of their professional obligations. Generally, professionals in leadership roles have obligations to declare any conflicts of interest, if they are unavoidable, to permit impartial colleagues to help manage the conflict. Unlike undue influence, which is about external pressure and its effect on decision-making, a conflict of interest arises from competing interests personal to the individual that have the potential to compromise objectivity.

Committee of Professional Conduct The body within the ICLA responsible for the establishment and advice on the Code of Professional Conduct, including the sub-committee responsible for the review and management of deviations from the Code.

Cybersecurity Cybersecurity is the art of protecting people, processes and technologies, including networks, devices, data and business processes, from unauthorized access or modification, or criminal use in support of the practice of ensuring confidentiality, integrity, and availability of information and systems.

Cybersecurity Communication A written, electronic, or oral communication issued by a member in support of cybersecurity practice. These may include professional reports, statements, or testimony, opinions, recommendations and assertions of cybersecurity posture and risks in addition to public facing communications including articles, blogs, white papers, conference presentations and keynotes, and social media communications.

Cybersecurity Information Information about cybersecurity. **Actionable cybersecurity information** is the subset of cybersecurity information that includes information about cybersecurity threats, attacks, and vulnerabilities to support the timely detection and response from a cybersecurity event and to limit and mitigate the scope and magnitude of such cyber events.

Cybersecurity Practice The practice of protecting an organization's business from cybersecurity threats.

Employer An entity or individual that directly compensates, hires, or engages an individual to perform work or services. This includes, but is not limited to, entities or persons who:

- Employ the individual as a full-time or part-time employee;
- Engage the individual as a contractor or independent consultant;
- Act as a client or organization for whom the individual provides services under any contractual arrangement; or
- Have a legal or contractual relationship that obligates the individual to perform work, regardless of classification or nomenclature.

For purposes of this Code, "Employer" covers any entity or person responsible for engaging the individual's services and providing compensation, regardless of the specific employment or contractual arrangement.

Fundamental Canons (or "Canons") The professional and ethical standards aligned with the Principles of the Code. Members must comply with the Canons in support of the Principles of the Cybersecurity Profession as part of the responsibility of the Association and its Members to the public.

Future Compensation Financial or other incentives provided in the present that may be realized at some point in the future, either short or long term, as the result of present-day actions. As an example, future compensation may result from an equity grant in an organization; an individual may use undue influence to promote that organization to secure their equity.

Information Sharing (for Collective Defense) Information sharing, as part of strategies for collective defense, involves the collection, analysis and sharing of actionable cybersecurity information, including threat information and strategies for protection, detection, response and recovery, across organizations for the defense of each organization and the wider community.

Law Statutes, regulations, judicial decisions, and other statements having legally binding authority over the Member or the Member's organization.

Member A dues-paying member in good standing of the International Cybersecurity Leadership Association (ICLA), at the level of General Member or above according to the ICLA's standards and processes.

Misinterpretation, Misquotation, Misuse of Information The reporting or recording of a subset of facts, data or information such that the initial and intended meaning is lost or no longer clear, leading to a change in the interpretation of the facts, data or information.

Must Must represents an obligation for compliance with the Code. **"Must"** is used to denote a mandatory obligation; compliance with these requirements is non-negotiable, unequivocal, and imperative. By contrast, **"Shall"** also represents an obligation, however, one where leeway is allowed in the approach to compliance, provided there is the appropriate documentation, rational explanation and justification of the Member's approach to compliance for this obligation.

May **"May"**, and its aligned term, **"Should"**, represent recommendations for compliance with the Fundamental Canons and Rules of Practice. Both **"May"** and **"Should"** do not create a binding requirement for conformance with the Code, instead providing guidance for alignment with the Code. **"Should"** is more prescriptive in that it denotes a recommendation or preferred course of action intended to ensure alignment with the intentions of the Code.

Principles The Code of Professional Conduct at its core is defined around six areas of basic, underlying rules and concepts that guide the actions and decisions of members of the ICLA:

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

Qualifications The combination of education, training, experience, skills, and credentials that an individual must possess to competently perform their professional duties.

Regulations Regulations are standards and rules adopted by administrative agencies to clarify their interpretation of a law, how a law will be implemented and how they will be enforced. This can be thought of as the means to define and enforce standards and best practices that should be in place to support the agency's interpretation of the law. Regulations often have the same force as laws, since, without them, regulatory agencies would not be able to enforce laws. As such, compliance with regulations is considered a legal obligation.

Rules of Practice The "Rules of Practice" (or "Rules") provide additional explanatory, educational, and advisory material on how the Fundamental Canons are to be interpreted and applied. The Rules provide guidance on the interpretation of the Canons and may be used to assert and confirm the reasonableness of behavior in compliance with a Canon. The Rules are designed to help members interpret and apply the principles of the code in various circumstances by offering additional context and examples. The Rules are defined and enumerated as annotations to the individual Fundamental Canons. There are no set number of Rules required for each Canon; Rules may be added over time based on the need for further guidance.

Undue Influence A situation of Undue Influence occurs when one party (including individuals and organizations) has (or has the appearance of having) power or influence that may be used to influence another party's decisions or actions inappropriately. This often implies pressure or manipulation, where the influenced party might make decisions that are not in their best interests or the best interests of their organization. Unlike a conflict of interest, which arises from competing interests that have the potential to compromise objectivity, undue influence is about external pressure and its effect on decision-making.

03 / SECTION

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, identified as Annotations, provide additional explanatory, educational, and advisory material on how the Fundamental Canons may be interpreted and applied for common situations where guidance may be required to meet the intent of the Canon and comply with the general Principles. Each Canon may have Rules of Practice for those situations where additional guidance is required.

PRINCIPLE 1

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

Members serve as positive examples within the cybersecurity profession and shall not commit any act that, in the determination of the ICLA, 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.

ANNOTATION 2.1

Members shall foster professional environments that are free from harassment, bullying, intimidation, retaliation, or other conduct that undermines the dignity and professional standing of others.

ANNOTATION 2.2

Members shall treat all individuals fairly and respectfully, and shall not engage in conduct that discriminates against, excludes, or disadvantages others in violation of applicable laws or organizational policies.

PRINCIPLE 2

Standards of Practice**FUNDAMENTAL CANON 3**

A member shall ensure that they have the appropriate education and/or experience, skills and knowledge for the tasks required for their role, consistent with guidance provided by the ICLA or other entities as applicable to the Member's role as a cybersecurity practitioner.

ANNOTATION 3.1

Members shall strive to stay current with practices and advances in cybersecurity.

ANNOTATION 3.2

Members must ensure they possess the appropriate skills and experience required for their area of responsibility, regardless of whether their role has specified minimum education or experience qualifications.

FUNDAMENTAL CANON 4

Members shall consistently and transparently disclose the current cybersecurity risks, threats and the adequacy of controls for the organization's stated risk tolerance, in accordance with internal policies, to the identified executive leadership team and relevant stakeholders within their organization.

ANNOTATION 4.1

Members are responsible for fair, accurate, timely and understandable description of cybersecurity risks, and the adequacy 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, and regulators as appropriate, for accuracy and completeness.

ANNOTATION 4.3

In the absence of an identified executive leadership team and relevant stakeholders within their organization, or where otherwise unable to disclose to said leadership, members shall disclose current cybersecurity risks, threats and the adequacy of controls for the organization's stated risk tolerance to their immediate management.

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 information exchange mechanisms, including, where possible, 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.

PRINCIPLE 3

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.

ANNOTATION 6.1

Members are encouraged to seek assistance from other professionals as needed in support of their role, provided that such professionals are bound by duties of confidentiality to their clients (the member) based on membership in their licensing body.

PRINCIPLE 4

Communications

FUNDAMENTAL CANON 7

Members shall take appropriate measures to ensure that their cybersecurity communications, whether written, electronic, or oral, are clear and appropriate to the circumstances and the intended audience.

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

When communicating on behalf of an organization on matters of an Employer's cybersecurity posture in public forums (such as conferences), members shall take reasonable steps to ensure the review of the communication by an appropriate member of that organization.

FUNDAMENTAL CANON 8

Members shall exercise diligence to ensure that their communications do not contain misrepresentations of fact or omit facts pertinent to the subject of the communication or otherwise comment 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 may offer opinions about events provided that their opinions are clearly identified as such, are not represented as statements of fact and do not disclose any confidential information.

PRINCIPLE 5

Conflict of Interest**FUNDAMENTAL CANON 9**

A member shall ensure their interests and relationships, including personal, professional or financial, do not interfere with the member's ability to make impartial decisions in their professional role (a Conflict of Interest), or have the potential to create the appearance of a Conflict of Interest, and when such actual or 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 with this Code and subject to applicable laws and legal obligations, including employer policies, and otherwise ensuring that:

- The Member has disclosed any actual conflict of interest or circumstances creating the potential appearance thereof to appropriate 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.

FUNDAMENTAL CANON 10

Members shall not solicit or accept direct or indirect compensation from more than one party in a related matter, 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 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, if applicable, the member's Employers' policies.

PRINCIPLE 6

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 impossible or not successful, the member may seek an opinion from the Professional Conduct Board.

ANNOTATION 12.1

If a Member believes that they may have violated the Code, the member should seek guidance from the Professional Conduct Board of the ICLA.

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 and seek counseling from the appropriate body of the Association, except where the disclosure would be contrary to law, or would divulge Confidential Information.

FUNDAMENTAL CANON 14

Members shall respond promptly, truthfully, and fully to requests for information by, and cooperate fully with, an appropriate counseling and disciplinary body of the Association in connection with any disciplinary, counseling, 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 13, 2026

04 / SECTION

Proposed Topic Areas

PROPOSED ADDITIONAL AREA	STATUS
AI Leadership Standards & Ethics	Not Started
Multiple Employment Conflicts of Interest	Not Started

05 / SECTION

Version History and Change Log

Version History

DATE	VERSION	PUBLISHED
October 13, 2026	v1.0	

Change Log

DATE	CHANGE	SOURCE OF CHANGE

06 / SECTION

Contributors

Initial draft versions, 0.0 to 0.9, of the Code were the result of the energy and experience from many individuals, including:

Rich Barreto

Joanna Burkey

Steve Crocker

Neil Daswani

Madhav Gopal

David Hirsch

Tyson Kopyczinski

Sounil Yu

Charles Blauner

Charisse Castagnoli

David B. Cross

Daniel B Garrie

Heather Hinton

Diana Kelley

Susanne Senoff

Steve Zalewski

We thank them for their initial and ongoing contributions.