Code of Professional Conduct

Integrity in action. Security in practice.
Protecting what matters most.

ISC2™

Table of Contents

About the Code of Professional Conduct

The Code of Professional Conduct (the "Code") establishes the foundation for what it means to serve the cybersecurity profession with integrity, competence, and accountability. It reflects a collective commitment to safeguarding the public, enhancing trust in the digital ecosystem, and maintaining the highest ethical and professional standards in the cybersecurity profession. More than a set of rules, this Code of Professional Conduct serves as a guide for informed decision-making, responsible actions, and continual growth, supporting both individual professionals and the broader cybersecurity community in advancing a safe and secure cyber world.

Guiding Principles

The Code's guiding principles are grounded in the long-standing canons of the **ISC2 Code of Ethics**. Developed to enhance - not replace - that foundation, offering clearer guidance and support for cybersecurity professionals.

Ethics

Integrity

Commitment to Honesty and Transparency

As part of your commitment to integrity, you are expected to uphold honesty and transparency in all areas of your work. These values build trust, support sound decisions, and enhance credibility.

Conflicts of interest happen when your personal interests, such as business, financial, family, or social factors, could influence your professional judgment or actions. These conflicts may be intentional or unintentional, but even the appearance of a conflict can damage trust and credibility. You are expected to recognize and disclose any actual or potential conflicts promptly so they can be managed properly.

Anti-bribery and corruption regulations are designed to uphold fair organizational practices and foster integrity and transparency. These regulations strictly prohibit offering, giving, or accepting anything of value such as gifts, entertainment, kickbacks, or other incentives to gain an unfair advantage. In your role, handling sensitive data and making critical organizational decisions requires heightened awareness of these regulations. When engaging with third parties or stakeholders, be vigilant about actions that could be perceived as improper, even if they are well-intentioned. If you are uncertain about a situation or suspect a possible violation, check your organization's policies or ask for guidance to make sure your actions remain ethical and compliant.

Commitment to the Profession

As professionals, we have a responsibility not only to our organizations and clients, but also to maintain the integrity and advance the profession itself. Your conduct directly impacts the reputation of the entire profession, so it is important to act honestly and responsibly in how you represent yourself and your work.

- Be honest and accurate when communicating your qualifications and experience.
- Misleading, deceptive, or false statements or claims about your professional qualifications, certifications, experience, or performance are unethical and erode trust.
- Cheating and other fraudulent exam practices are strictly prohibited. They undermine the integrity of the certification, jeopardizing your career and the reputation of the certification program.

Commitment to Responsible Use of Privileges

You have an important responsibility that comes with elevated access and insights into security systems. Professionals granted privileged access must use it only for authorized and legal purposes. To uphold this trust, avoid actions that could compromise security, such as accessing data outside the scope of your role, sharing credentials, or improperly escalating privileges. If you become aware of any misuse, unnecessary privileges, or threats, report them through the proper channels.

Confidentiality

Commitment to Data Security and Privacy

Maintaining confidentiality is fundamental to your role. This responsibility includes handling various types of data, including private, proprietary business, and regulated data. Unauthorized disclosure of this data can lead to serious consequences and potentially cause significant harm to individuals and organizations. Implement processes such as proper data classification, encryption, access controls, awareness training, and data protection measures to help protect confidentiality and prevent mishandling of data. In addition to technical measures, attention must also be given to human factors such as social engineering risks, phishing attempts, and careless data handling during daily operations. A proactive approach is key to reducing risks and ensuring the security of sensitive information.

Respect for Laws and Regulations

Commitment to Compliance and Your Organization's Code of Conduct

Adhering to all applicable laws, regulations, and organizational policies is a foundational expectation, regardless of your role or level of authority. Upholding legal and ethical standards enhances accountability, fosters trust, promotes transparency, and strengthens overall security. Always act in accordance with your organization's code of conduct and refrain from engaging in any actions that may compromise compliance. Be especially vigilant for attempts to manipulate, misrepresent, or conceal information; activities that could be considered fraudulent or illegal; and situations where ethical boundaries may be at risk. If you become aware of any potential violations, report them promptly using your organization's established reporting channels.

> *"Always act in accordance with your organization's code of conduct and refrain from engaging in any actions that may compromise compliance."*

Public Safety and Societal Impact

Commitment to Security and Risk Reduction

You are responsible for identifying risks, promoting secure practices, and helping others understand their roles in protecting systems, data, and people. Failure to uphold security can put organizations and society at risk. To mitigate this, it is essential to communicate effectively, leverage data to inform decisions, and lead by example. Your ongoing efforts to educate, collaborate, and foster trust help create a culture where security is everyone's responsibility.

Commitment to Responsibly Securing Emerging Technologies

Lead efforts to adopt a proactive approach for maintaining sound security and ethics in the deployment and use of emerging technologies such as artificial intelligence (AI), quantum computing, blockchain, and other fast-evolving innovations. Before implementing these technologies, advocate for initiatives that establish governance measures to promote responsible and ethical practices. This includes:

- Conducting needs analyses, defining scope, performing due diligence, and implementing security controls.
- Emphasizing accountability, bias mitigation, privacy, security by design, strong security governance, and responsible decision-making.
- Building awareness and providing ongoing training about ethical considerations, responsible use of emerging technologies, and potential risks.

Forward-thinking practices help ensure all stakeholders are aligned in prioritizing security and ethics throughout the technology's lifecycle.

Professional Conduct

Responsibility and Accountability

Commitment to Balancing Security & Organization Objectives

You work with organizational leaders to enable them to meet their goals. You help the organization move forward with its objectives while protecting people, clients, and data. Building cybersecurity into the organization from the beginning keeps costs and risks down. Flexibility and understanding what each organization needs are important. A strong cybersecurity culture protects the organization and enhances its reputation, operational resilience, and long-term success.

Commitment to Employers, Employees, and Stakeholders

Your primary responsibility is to protect human life by safeguarding systems that, in some cases, may have a real-world impact on human safety and stakeholder data, including that of your organization, clients, and third parties. While supporting organization objectives, it is crucial to maintain the trust placed in you. This involves never bypassing protocols, concealing risks, or doing anything that could compromise security. You should clearly communicate risks, escalate concerns, and document decisions to ensure accountability.

Collaboration and Teamwork

Commitment to Respect for Others

Working with various teams and stakeholders, your ability to collaborate respectfully is essential to strong security. This includes valuing diverse perspectives, engaging others with professionalism, and fostering an environment where everyone feels included and heard. Approaching interactions with curiosity, clarity, and respect enhances teamwork, expands insight, and reinforces security and ethics. By contributing constructively and speaking up when necessary, you help build a stronger team and advance the profession as a whole.

Commitment to Ethical Leadership & Workplace Culture

What you do is more than your title. You lead by example, showing integrity, accountability, and good judgment in your daily work. By communicating clearly, especially when discussing risks, you earn trust and help create a culture that values and prioritizes security.

Competence and Continuous Improvement

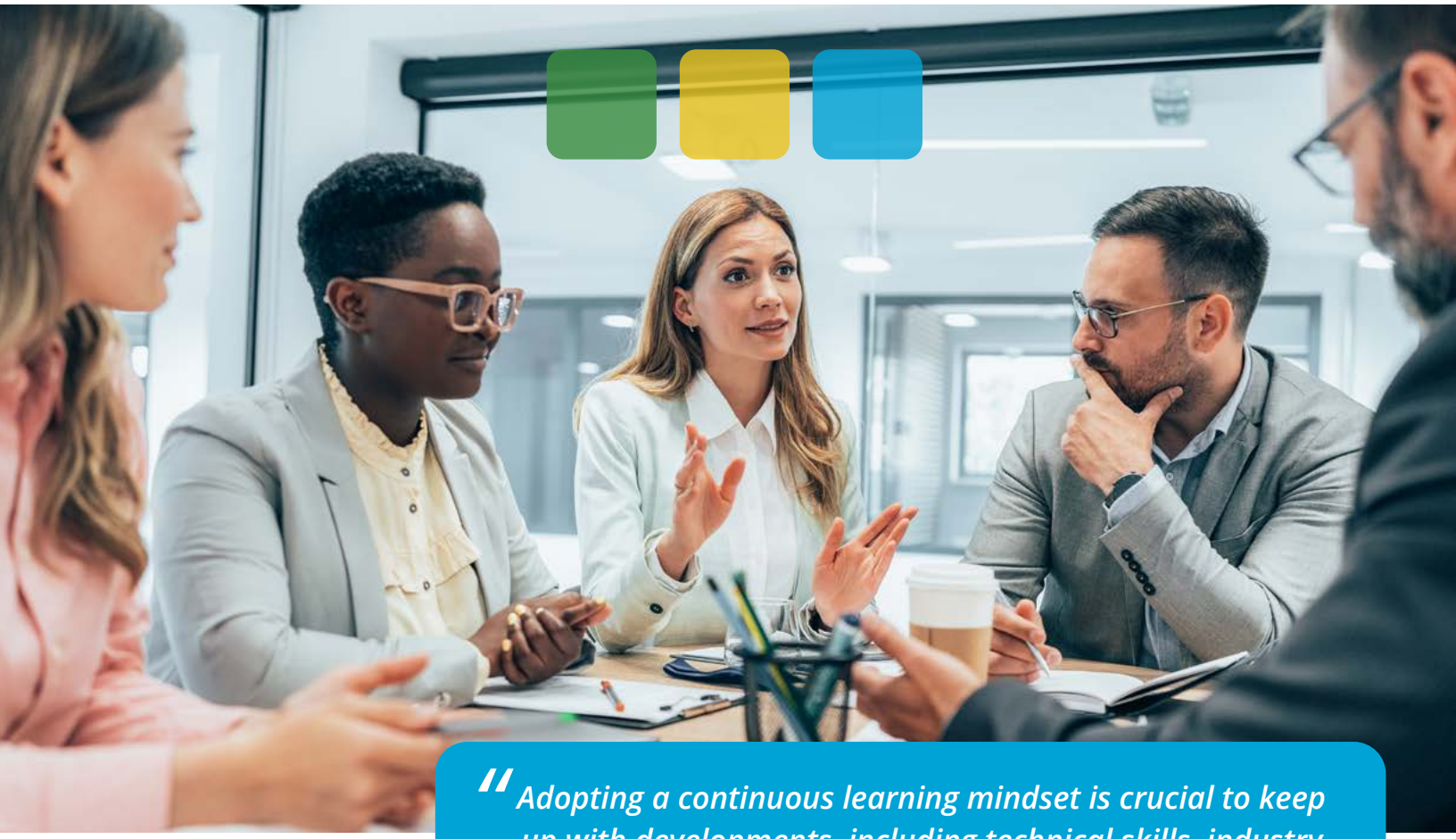
Commitment to Competence and Continuous Improvement

The cybersecurity industry is complex and constantly changing. To ensure you provide services in your areas of expertise, be honest and transparent about the areas you are qualified for in all situations and communicate any limitations in your education, training, and experience. Adopting a continuous learning mindset is crucial to keep up with developments, including technical skills, industry practices, and new regulations. Explore other growth opportunities, like mentoring, community outreach, sharing knowledge, attending conferences, and participating in other professional areas.

Reporting Issues and Concerns

Commitment to Ethical Reporting

You have a responsibility to report any security vulnerabilities, compliance violations, insecure practices, and unethical behavior that could put organizations, individuals, or the public at risk. By raising these concerns, you help mitigate risks and address issues before they escalate, fostering a safer and more ethical environment. Familiarize yourself with your organization's designated reporting channels (e.g., ethics hotline, Human Resources, Compliance Officer, etc.), which will vary by industry and region. Bringing forward concerns about organizational activities or ethical, compliance, or conduct issues is vital to help drive transparency, reduce risk, and create a culture of integrity.



> *"Adopting a continuous learning mindset is crucial to keep up with developments, including technical skills, industry practices, and new regulations."*

Bringing the Code to Life

To support your commitment to ethical and professional conduct, we offer a range of helpful tools, resources, and guidance to assist you in applying the Code in everyday situations. Feel free to visit **ISC2.org/about/Code-of-Professional-Conduct** to discover the story behind the Code's development and explore additional materials that bring the Code to life. These resources are designed to help you feel confident in navigating ethical challenges at any stage of your professional journey.

How to Get Involved

We are constantly enhancing this program and invite cybersecurity professionals to contribute. If you are interested in **volunteering**, sharing your expertise, or assisting in developing future ethics and conduct resources, we welcome your participation.

Contact us at **codeofconducttaskforce@isc2.org** to get involved and help shape what's next.

"Integrity in action. Security in practice. Protecting what matters most."

Code of Professional Conduct

About ISC2

ISC2 is the world's leading member organization for cybersecurity professionals, driven by our vision of a safe and secure cyber world. Our more than 265,000 certified members, and associates, are a force for good, safeguarding the way we live. Our award-winning certifications – including cybersecurity's premier certification, the CISSP® – enable professionals to demonstrate their knowledge, skills and abilities at every stage of their careers. ISC2 strengthens the influence, diversity and vitality of the cybersecurity profession through advocacy, expertise and workforce empowerment that accelerates cyber safety and security in an interconnected world. Our charitable foundation, **The Center for Cyber Safety and Education**, helps create more access to cyber careers and educates those most vulnerable. Learn more, get involved or become an ISC2 Candidate to build your cyber career at **ISC2.org**. Connect with us on **X**, **Facebook** and **LinkedIn**.