C3

Cybersecurity Credentials
Collaborative

C3 MEMBERSHIP APPLICATION

ORGANIZATION INFORMATION

Organization Name: ______________________________

Organization Address: ______________________________

____

Organization Website:______________________________

Organization Business Focus:______________________________

CONTACT INFORMATION

Individual’s Name and Title:______________________________

____

Email address:______________________________

Phone number:______________________________

APPLICANT PROFILE

List your goals and a description of the certifications that are offered through your organization?

Provide a history of your organization? How many years in practice (Minimum of 3 years or Vote)?

How many certified holders do you have and length of period each certification has been in existence (Must have Minimum of 20,000 Certified Holders Total/ Minimum Three Years in Existence for Non-Vote)?

Why do you consider your certification to be an industry standard in the cybersecurity industry?

UNIFIED PRINCIPLES OF PROFESSIONAL ETHICS IN CYBER SECURITY AGREEMENT

To be considered for C3 membership all applicant organizations must agree to abide by the Unified Principles of Professional Ethics in Cyber Security listed created and adopted by the C3 (as listed on the C3 website). Please indicate below that your organization can fully agree to and abide by the professional ethics principles as described; as well provide a reference for your organization's ethics policies.

____

____

____

____

LEGAL DISCLOSURE INFORMATION

We ask that all applicants fully disclose any cases involving their organization, pending or decision rendered, for review as applicable to the C3 Principles of Professional Ethics in Cyber Security and as related to C3 brand reputation within our industry. If no litigation exists please just list N/A.

____

____

____

____

PLEASE SELECT ONE OF THE FOLLOWING:

□ Member - Annual Dues US $5,000

In order to be a voting member, the applicant organization must have a vendor neutral, ISO/ANSI/IEC 17024 accredited credential within the information security, privacy or related IT field.

I,______________________________(individual's name), Representing ___________________________________ (name of organization) agree to the Unified Principles of Professional Ethics in Cyber Security available at www.cybersecuritycc.org. _ As well, I agree to the accuracy of the legal disclosure information listed above.

Please email a scanned copy of this completed application to the current President of the C3 as listed on the website.

Membership requires C3 Board majority approval. You will be contacted after formal Board review of your application. You also agree to a potential audit and to be contacted with any additional questions or concerns. Upon application approval, you will be invoiced for the annual dues.

Signature:____Date: ___________________________

Internal Use Only:
Received date:

Interview date:

Approved

date:

APPENDIX A
ETHICS POLICY

The Cybersecurity Credentials Collaborative (C3) and its member organizations have adopted A Unified Principles of Professional Ethics in Cyber Security, adapted from the Unified Framework of Professional Ethics for Security Professionals, originally set forth by the Security Professionals Ethics Working Group. In addition to C3 member organizations, the Unified Principles of Professional Ethics in Cyber Security have also been formally endorsed by ISSA. ISSA was one of the original participants in the Security Professionals Ethics Working Group.

Integrity

- Perform duties honorably, justly and responsibly, in accordance with existing laws, exercising the highest moral principles.
- Act in the best interests of stakeholders
- Refrain from activities that would constitute a conflict of interest.
- Report ethical violations to the appropriate governing body in a timely manner.

Objectivity

- Perform all duties in a fair manner and without prejudice.
- Exercise professional judgment in order to provide unbiased analysis and advice.
- When an opinion is provided, note it as opinion rather than fact.

Confidentiality

- Respect and safeguard confidential information and exercise due care to prevent improper disclosure.
- Maintain appropriate confidentiality of proprietary and otherwise confidential information encountered in the course of professional activities, unless such action would conceal or result in the commission of a criminal act.

Professional Competence

- Perform services diligently and with professionalism.
- Render only those services for which you are fully competent and qualified.
- Recognize and acknowledge the contributions of others.
- Refrain from professional misconduct which would damage the reputation of the profession.
- Participate in professional development activities to maintain the skills necessary to function effectively.

Consistent with the Unified Principles of Professional Ethics in Cyber Security which have been adopted by The Cybersecurity Credentials Collaborative (C3) and its member organizations, C3 member organizations are committed to encouraging self-reporting of adjudicated ethics violations by credential holders to the credential holder's employer and to other certifying bodies that have issued credentials to the individual. Also consistent with the Unified Principles of Professional Ethics in Cyber Security, C3 member organizations, as allowed by their respective policies and applicable law, may share results of finally adjudicated ethics violation complaints and the disciplinary measures imposed with other C3 member organizations.