Central Vigilance Commission C-O-C No. 5977735653
Licence No. 124161, Section 8(1) Act 2013, Ministry of Corporate Affairs, Government of India
TM, Section 23 (2), Rule 56 (1), TM No. 4123372 Dated 20-3-2019, Government of India

WWW.COUNCIL.ORG.IN

साइबर सतर्कता और सुरक्षा कार्यान्वयन परिषद

Council of Cyber Vigilance and Security Enforcement

AN AUTONOMOUS NON GOVERNMENT ORGANISATION

SERVICE | SAFETY | SECURITY | SYNERGY

Regional Office
497, 3rd Floor, CCIT Building,
Model Town, Ludhiana City,
Punjab - India PIN 141002
Contact: +91-7068710000
info@council.org.in

About Council

Council plays a catalytic role to reduce harm from cyber crime targeted at government establishments, national information resources, corporates and their customers and individuals. Through effective collaboration with our affiliates and member organisations and with the support of respective governments, we look at ways to provide practical assistance to law enforcement agencies and governments to protect critical national information infrastructures and individuals nationwide. Our operations take place in the form of projects and programs implemented time to time.

Council affiliates wide variety of stakeholders in the cause of cyber security from government and private sector such as research organisations, security agencies, banking and financial sector organisations, large corporates, SMEs and Start-ups, universities, educational institutions, end-users, operators, clusters and association as well as local, regional and national organisations.

Vision

A cyber-safe and secure India where everyone can use the cyber space and internet connected devices with confidence. A cyber space that is safe and secure for individuals, corporates, government establishments, national information resources. There is widespread availability and easy accessibility to a reliable and dependable system that offers education, training, development, and career preparation, catering to the interests and needs of all individuals seeking such opportunities. A world-leading cyber security workforce of professional samurais protects national information infrastructures, organizations, companies, and individuals, contributing to a digitally resilient society.

Mission

Our mission is to contribute for a cyber-safe and secure India, empowering individuals in utilizing the cyber space and internet-connected devices confidently. We endorse a trusted cyber environment for individuals, corporates, government establishments, and national information resources. Through widespread availability and easy accessibility, we offer a reliable system for comprehensive cyber security education, training, development, and career preparation. Our focus caters to diverse interests, enhancing skills and knowledge in the cyber security realm. We contribute in building a world-leading cyber security workforce of professionals, safeguarding national information infrastructures and contributing to a digitally resilient society. Together, we empower every citizen with tools, knowledge, and support, ensuring a confident navigation of the digital landscape for a cyber-safe and secure India.

Objectives of Council

1. To ensure an environment and culture of safety and security in cyber space through structure of training, vigilance and security enforcement through community participation.

2. To ensure, continuous awareness among society for cyber vigilance, safety and security in cyber space. This is accomplished through on-going training and development of ever-increasing number of people through non-formal and informal system and structures using online mode or instructor led off-line mode.

3. To promote best practices of training and development in cyber security field. To monitor expansion or growth training providing institutions and skilled manpower for implementation of techniques and technologies for safe and secure society and country in cyber space.

4. To support and provide a common platform for academic and technical education institutions to create and update effective curriculum for their courses and programs delivered through schools, colleges and universities related to the cyber security. The objectives are to expand competent and expert force for security of country in cyber space.

5. To ensue, a culture of usage of cyber space with peace and harmony to ensure unity in diversity of the country, to promote etiquettes and manner of usage of cyber space for information exchange and social media such that it evolves the prime values and principle of our country and discourage or illuminates anything which is against our country and unity in diversity. In other words, there is established culture of promoting, inspiring, encouraging and empowering contents for every citizen to build a healthy and wealthy and nation.

6. To ensure, presence of sufficient expertise and service providers in the country such that every individual or organization is safe and secure from the threats in the cyber space. There must be decline in the rising cyber fraud, or cyber-attacks or other crimes in cyber space.

Quality Policy

The Council of Cyber Vigilance and Security Enforcement is committed to achieving the highest standards of cyber security training and development and fostering a culture of safety and awareness in the digital landscape. We are dedicated to supporting the growth of cyber security education, reducing instances of cyber fraud and cybercrimes by creating awareness, promoting a culture of responsible cyber space usage, enhancing cybersecurity, contribute in building a competent cyber security workforce, and delivering tangible results through various projects implementation.

We actively promote participation in our comprehensive training courses and awareness initiatives in the field of cyber security through online and offline channels. By continually monitoring and improving our work, we demonstrate our unwavering commitment to excellence in cyber security. Our goal is to raise awareness, safeguard individuals and organizations, and contribute to the overall security of our nation in the digital era.

Quality Objectives

1. To provide high-quality cyber security training and development programs those meet or exceed industry standards.

2. To continually enhance the effectiveness of our cyber security education initiatives through regular evaluation and improvement processes.

3. To actively contribute to the reduction of instances of cyber fraud and cybercrimes by creating awareness and promoting safe practices.

4. To foster a culture of responsible cyber space usage by promoting ethical practices, peace, and harmony in the digital landscape.

5. To continuously enhance our cybersecurity measures and expertise to stay ahead of emerging threats and protect individuals and organizations.

6. To actively contribute to the development of a competent cyber security workforce through collaboration with educational institutions and industry partners.

7. To deliver tangible and impactful results through the successful implementation of various projects aligned with our objectives.

Quality Principles

Safety and Security: Ensuring the cyber space is safe and secure for individuals, corporates, government establishments, and national information resources.

Proactive Risk Management: We employ proactive risk management practices to identify, assess, and mitigate cyber security risks effectively.

Continuous Learning and Development: We foster a culture of continuous learning and development to ensure our team stays abreast of the latest cyber security trends, technologies, and best practices.

Stakeholder Engagement: We actively engage with our stakeholders to understand their needs, expectations, and feedback, and incorporate their insights into our programs and initiatives.

Collaboration and Partnership: Collaborating with affiliates, member organizations, and governments to effectively address cyber security challenges.

Accessibility and Inclusivity: Making comprehensive cyber security education, training, development, and career preparation accessible to all individuals.

Performance Measurement and Evaluation: We establish robust performance measurement systems and regularly evaluate our outcomes to drive continuous improvement and demonstrate the effectiveness of our work.

Innovation and Adaptation: We encourage innovation and embrace emerging technologies and methodologies to stay ahead of cyber threats and deliver cutting-edge solutions and training programs.

Excellence and Expertise: Striving to build a world-leading cyber security workforce, promoting best practices, and continuous professional development.

Continuous Improvement: Adapting and improving operations, programs, and initiatives to stay ahead of emerging cyber threats and challenges.

Key Performance Indicators (KPIs) for the "Council of Cyber Vigilance and Security Enforcement" based on the provided information:

1. Financial Aid Utilization: Monitor the utilization and effectiveness of financial aid. To recommend, support and provide aid to internship program participants pursuing higher education in leading universities, tracking the number of individuals supported and their academic achievements.

2. Reduction in Cybercrime Instances: Monitor the decline in cyber fraud, cyber-attacks, and other cybercrimes in the country as an indicator of the organization's impact on improving overall cyber security.

3. Cyber Culture Index: a. Develop a metric to assess the establishment and growth of a culture of cyber space usage that promotes peace, harmony, unity in diversity, and adherence to ethical practices.

b. Monitor the projects those impact factors such as the prevalence of positive and empowering online content, citizen engagement in promoting cyber etiquettes, and the overall perception of cyber space as a safe and inclusive environment.

4. Cybersecurity Effectiveness: a. Evaluate the effectiveness of the organization's efforts in ensuring the presence of sufficient expertise and service providers to enhance cybersecurity.

b. Measure the decline in cyber fraud, cyber-attacks, and other cybercrimes through metrics such as the number of reported incidents, successful prevention or mitigation of attacks, and the overall improvement in the security posture of individuals and organizations in the country.

5. Curriculum Development and Adoption: a. Monitor the number of academic and technical education institutions that utilize the common platform provided by the council to create and update effective curriculum for their courses and programs related to cyber security.

b. Shortlist the colleges, universities and institutions and their faculty for acknowledgement, appreciation and honour for ensuring and adopting up-to-date curriculum. The objective is to ensure the expansion of a competent and expert workforce in the field of cyber security, contributing to the vigilance and security of the country in the cyber space.

6. Trainers' Program Effectiveness: Evaluate the outcomes of the "Training of Trainers" program by assessing the number of qualified trainers produced, their ability to effectively train others in the field of cyber security, and feedback from program participants.

7. Project Implementation and Impact: Assess the successful initiation, implementation, and completion of projects aligned with the organization's objectives, measuring factors such as project completion rate, impact on cyber security awareness, and the effectiveness of implemented solutions.

8. Training Participation: Measure the number of individuals participating in the organization's comprehensive training courses and programs on cyber and information system security.

9. Awareness Reach: Track the reach and impact of awareness initiatives by monitoring the number of individuals reached through training, workshops, seminars, online courses, and social media campaigns.

10. Accreditation Success Rate: Evaluate the percentage of training centres that successfully receive accreditation from the organization for offering courses in the field of cyber security and ethical hacking.

11. Online Learning Platform Engagement: Assess the level of engagement and utilization of the organization's online learning platform, including metrics such as user registrations, course completion rates, and user satisfaction feedback.

12. Seminar Attendance and Online Awareness Course: a. Measure the attendance and participation in workshops and seminars conducted by the organization to create awareness of cyber laws and promote safe practices among teachers and students.

b. Assess the percentage of teachers and students who successfully complete online courses on cyber laws and precautionary measures against cyber threats and vulnerabilities.

13. Internship Program Outcomes: Evaluate the success of the internship programs by monitoring the number of participants, their feedback and satisfaction, and their subsequent career advancement in the field of cyber security.

Reason for Existence:

The Council of Cyber Vigilance and Security Enforcement exists to fulfill the vision of India as cyber security super power and creating a cyber-safe and secure environment. The organization recognizes the increasing threats posed by cybercrime and aims to reduce harm to government establishments, national information resources, corporates, and individuals. By collaborating with affiliates, member organizations, and governments, the Council provides practical assistance for creating awareness and establishing training and development system to generate competent and professional workforce.

The organization's operations take the form of projects and programs, implemented over time, to address evolving cyber threats. The Council affiliates a wide variety of stakeholders, including government and private sector entities, research organizations, security agencies, banking and financial sector organizations, corporates, SMEs, universities, educational institutions, end-users, operators, clusters, and associations.

Council is dedicated to ensuring widespread availability and easy accessibility to a reliable system that offers comprehensive education, training, development, and career preparation opportunities in cyber security. By building a world-leading cyber security workforce, the organization contributes to a digitally resilient society and contributes to protect national information infrastructures, organizations, companies, and individuals. By raising awareness, safeguarding individuals and organizations, and contributing to the overall security of the nation in the digital era, the organization plays a vital role in protecting critical information, promoting ethical cyber practices, and ensuring the safety and well-being of the digital community.

Overall, the Council's reason for existence is to empower individuals, enhance cyber security awareness, promote best practices, and create a safe and secure cyber space that fosters the growth and prosperity of India.