NATIONAL CYBER SECURITY RESEARCH & DEVELOPMENT (NCSR&D) CENTRE (IEC - MATERIAL)

राष्ट्रीय साइबर सुरक्षा मानक

NATIONAL CYBER SECURITY STANDARDS

A SELF-GOVERNING ORGANIZATION

www.ncdrc.co.in

ABOUT National Cyber Security Standards

About National Cyber Security Standards

In today's interconnected world, cybersecurity threats are not only sophisticated but also pervasive. The National Cyber Security Standards (NCSS) play a crucial role in safeguarding our nation's digital space from these evolving threats, ensuring the security and resilience of our virtual environment.

To combat the multifaceted nature of cyber threats, a comprehensive and standardised approach to security is essential. NCSS develops and implements policies and procedures that address the diverse spectrum of cyber risks. These standardised protocols ensure consistency, reliability, and effectiveness in combating threats, thereby enhancing overall cybersecurity posture.

NCSS envisions a secure digital future for India. By fostering education, awareness, and research, we empower citizens and organisations to defend against cyber threats. Our goal is to create a resilient digital environment where innovation can flourish safely. The NCSS operates within the $185.7 billion cybersecurity market, addressing the critical demand for skilled professionals and research infrastructure.

Mission

Our mission at the National Cyber Security Standards (NCSS) is clear: to establish India as the Cyber Security Capital by 2035.

About National Cyber Security Research & Development Centre

The National Cyber Security Research & Development Centre (NCSRDC) is a premier institution committed to advancing the field of cybersecurity in India through pioneering research, innovative technology development, and strategic collaboration. As the digital landscape continues to evolve, the threats to national security and critical infrastructure have become more sophisticated and pervasive. In response to these challenges, the NCSRDC plays a vital role in fortifying the nation's cyber defences and ensuring a resilient digital environment.

LEARNING

- Cyber Threats that affect your institution
- Industry best practices on Cyber Security to protect your organizations critical infrastructure
- Improve internal efficiency and output of your organization

NETWORKING

- Networking opportunities with Indian and Global Security Experts / Professionals
- To showcase to the the Industry, your environment and skill of staff

SHARING

- Share your best Cyber Security practices with other member
- Enhace Cyber Security of Nation / Industry / Institution/ Indivuduals

MESSAGE

SHRI. NARENDRA MODI
Hon'ble Prime Minister of India

"Starting from the stone age, it has always been the human psyche to protect itself from external threats. The ideas, tricks, and methodologies of protection from evil and intruding threat factors have also evolved over time. Initially, we, the humans, had to guard ourselves against physical threats like invaders and looters. Nowadays, with the rising popularity of cyber connectivity and worldwide interlinking, the evil has also evolved in the form of breaches of cyber security. It is a virtual world we have created, and we have to be well-prepared to protect and sustain our virtual world from virtual invaders.

I am really happy to learn that the National Cyber Safety & Security Standards is thinking about the possible solutions and establishing norms against Cyber Crimes. The hope is that this handbook will be a ready reckoner on matters related to cyber protection in our country. I hope the initiatives of National Cyber Safety and Security Standards will establish and convey the most effective ways and means of protecting our National Security against the worst sort of cyber attacks and provide the best safeguards against the cyber criminals threatening our Nation and its Integrity. I wish all the success to the National Cyber Safety and Security Standards in its crusade to protect the Nation."

EXECUTIVE COUNCIL MEMBERS

Dr. G.A. Rajkumar IAS(R)
Former Additional Chief Secretary to Government
Chairman - National Cyber Security Standards, New Delhi

Lt. Gen. Arun Kumar Sahni, PVSM, UYSM, SM,VSM
Former General Officer Commanding in Chief - Indian Army
Chairman - Research & Development Council, NCSS.

Lt. Gen. R K Anand, AVSM, SM, VSM(Retd)
General Officer Commanding (GOC) of Dakshin BharatArea, Indian Army.
Chairman - National Advisory Council, NCSS

Dr. S.S. Mantha
Former Chairman All India Council for Technical Education(AICTE), New Delhi
Chairman - National Technical Council, NCSS.

CORE OBJECTIVES:

The NCSRDC's mission is to safeguard India's digital infrastructure by:

- Conducting Cutting-Edge Research: The Centre focuses on identifying and mitigating emerging cyber threats through comprehensive research. This includes developing advanced cybersecurity technologies, tools, and methodologies that address both current and future challenges.
- Innovative Technology Development: Leveraging the latest technological advancements, the Centre is at the forefront of creating state-of-the-art cybersecurity solutions that enhance the security posture of critical infrastructure and digital assets.
- Strategic Collaboration: The NCSRDC fosters partnerships with industry leaders, academic institutions, and international bodies. These collaborations are crucial for creating a unified and coordinated response to cyber threats, ensuring that India remains ahead in the global cybersecurity landscape.

Key Focus Areas: The NCSRDC is dedicated to several key areas critical to national cybersecurity:

1. Threat Detection and Mitigation: Developing advanced systems and methodologies for detecting, analysing, and mitigating cyber threats before they can cause significant harm.

2. Cyber Defence Strategies: Crafting comprehensive defence strategies that protect national digital infrastructure from sophisticated cyber-attacks.

3. Cybersecurity Policy Advisory: Providing expert advice to government agencies on the formulation and implementation of robust cybersecurity policies and frameworks.

4. Training and Capacity Building: Offering specialised training programs aimed at building a highly skilled cybersecurity workforce capable of tackling the most complex cyber challenges.

5. Research and Innovation Grants: Facilitating research and innovation by providing grants and funding to academic institutions and research bodies, fostering a culture of continuous improvement and advancement in the field of cybersecurity.

6. International Collaboration: Partnering with global cybersecurity organisations and research institutions to exchange knowledge, adopt best practices, and ensure compliance with international standards.

NATIONAL IMPACT

The NCSRDC's work is pivotal in addressing the growing demand for cybersecurity professionals in India. With the country needing approximately 3 million cybersecurity experts by 2030, the Centre's initiatives are geared towards closing this gap by establishing 100 National Cyber Security Research & Development Centres across India by 2027.

This Network of Centres Will Play a Crucial Role in:

- Bolstering National Security: By securing critical infrastructure and sensitive data from cyber threats, the NCSRDC enhances the nation's overall security posture.
- Supporting the Corporate Sector: With 78% of the corporate sector currently reporting a shortage in cybersecurity staff, the NCSRDC's training and capacity-building programs are essential in meeting industry demands and ensuring that businesses can protect their assets effectively.
- Driving Economic Growth: The cybersecurity market is a burgeoning $185.7 billion industry, and the NCSRDC's efforts in research, innovation, and skill development contribute significantly to this sector's growth, positioning India as a global leader in cybersecurity.

BENEFITS FOR INSTITUTION

- **Academic Council Membership:** The Principal or any nominated member from the institution will be appointed as a distinguished member of the Academic Council.
- **Accredited e-Certificate:** Institutions will receive an accredited e-Certificate.
- **Authorized NCSS Logo Usage:** With prior approval, the NCSS logo can be displayed on your website or promotional materials.
- **NCSS-CPE Credits:** The NCS R&D Centre confers an entitlement to 2 NCSS-CPE credits.
- **Additional NCSS-CPE Credits:** Additional credits can be acquired by participating in further courses, summits, or specialized programs.
- **Discount on Courses:** Institutions can avail of a 30% discount on Cyber Security courses.
- **Certification:** The Annual Cyber Security Audit Certificate can be submitted to competent authorities like AICTE, UGC, NAAC, NBA, NMC, etc., during their annual review process.

Industry Expectations from Cyber Security R&D Centre: The industry holds high expectations from the R&D centre, which include:

- Conducting research that leads to innovative cybersecurity technologies, tools, and methodologies.
- Identifying and mitigating emerging cybersecurity threats relevant to the industry.
- Co-developing projects where industry and academia collaborate to solve complex cybersecurity challenges.
- Developing training programs and internships that prepare students and professionals with necessary skills.
- Providing access to expert researchers and academics for consultancy on cybersecurity issues.
- Delivering tangible results, such as patents, research publications, and deployable cybersecurity solutions.
- Developing new cryptographic protocols and techniques to enhance data encryption, integrity, and secure communications.
- Creating automated tools for continuous vulnerability assessment, penetration testing, and security audits.
- Implementing AI and machine learning models for predictive analytics, anomaly detection, and automated threat response systems.
- Collaborating on the integration of security measures throughout the software development lifecycle, including secure coding practices and automated security testing.

Annual Cyber Security Audit Certification

The National Cyber Security Standards Annual Cyber Security Audit Certification is a mandatory assessment for the National Cyber Security R&D Centre. This certification ensures that the center consistently adheres to the highest standards of cybersecurity, maintaining a secure and compliant environment for research and development activities. By undergoing this rigorous annual audit, we demonstrate our unwavering commitment to protecting sensitive data, mitigating cyber risks, and upholding the integrity of our operations.

ROLES AND RESPONSIBILITIES OF INSTITUTION

1. Infrastructure Support:

- Provide the necessary infrastructure, including laboratories, hardware, and software, required to establish and maintain the NCS R&D Centre. (Mostly the available resource will be utilised.)
- Ensure the availability of a secure and conducive environment for research activities and data protection.

2. Academic Integration:

- Integrate cybersecurity research and development as part of the institution's digital culture.
- Encourage faculty and students to actively participate in the research initiatives led by the NCS R&D Centre.

3. Collaboration and Networking:

- Foster collaboration between the institution, industry partners, and other academic entities to enhance research outcomes and practical applications.
- Participate in national and international cybersecurity forums, workshops, and conferences to promote the institution's involvement in cybersecurity advancements.

4. Data Sharing and Compliance:

- Ensure compliance with all NCSS protocols, including regular data sharing and reporting as required for research and audit purposes.
- Maintain strict adherence to confidentiality agreements and data protection regulations.

5. Faculty and Student Involvement:

- Form a Cyber Security Committee to lead and oversee the activities of the Digital Space of your institution.
- Encourage students to engage in research projects, internships, and training programs associated with the NCS R&D Centre.

6. Sustainability and Growth:

- Commit to the continuous development and expansion of the NCS R&D Centre by securing funding, grants, and resources from Government and Industry
- Regularly review and update the institution's cybersecurity strategies to align with emerging threats and technological advancements.

7. Promotion and Outreach:

- Promote the achievements and research outcomes of the NCS R&D Centre through publications, seminars, and media channels.
- Engage with the local and global community to raise awareness about the importance of cybersecurity and the role of the NCS R&D Centre in fostering a secure digital future.

PREVIOUS EVENT GALLERY

राष्ट्रीय साइबर सुरक्षा मानक

NATIONAL CYBER SECURITY STANDARDS

A SELF-GOVERNING ORGANIZATION

NATIONAL CYBER SECURITY STANDARDS
New Delhi.
Ph : 011-6934 3799   Email: support@ncdrc.co.in
www.ncdrc.co.in

PARTICIPATE • PERFORM • PROTECT